


the dtic

 Department:
 Trade, Industry and Competition
 REPUBLIC OF SOUTH AFRICA

TENDER NO.: RFP002-2025/26

APPOINTMENT OF A **CONTRACTOR** FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)

INVITATION DATE	: 12 December 2025
BRIEFING SESSION DATE	: 15 th January 2026
TIME	: 10H00
VENUE	: Rainprop office the dtic campus

FAILURE TO ATTEND THE BRIEFING SESSION WILL INVALIDATE THE TENDER OFFER

TENDER CLOSING DATE & TIME	: 29 th January 2026@ 11am
TENDER OPENING DATE & TIME	: 30 January 2026 @ 11am
TENDER VALIDITY	: 120 CALENDER DAYS

TENDERER'S NAME	:	_____
MAILING ADDRESS	:	_____
TELEPHONE NUMBER	:	_____

I certify that this Tender is made without prior understanding, agreement, or connection with any corporation, firm or person submitting a Tender for the same materials, supplies or equipment and is in all respects fair and without collusion or fraud. I agree to abide by all conditions of this Tender and certify that I am authorised to sign this Tender.

 AUTHORISED SIGNATURE

 PRINT NAME

Sealed documents marked "APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26) must be dropped off in the tender box situated in the Rainprop Offices (Block B, DTIC Campus) before stipulated time.

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)

TABLE OF CONTENTS

<u>PART NO.</u>	<u>DESCRIPTION</u>	<u>COLOURS</u>	<u>PAGE</u>
	THE TENDER		
PART T1	TENDERING PROCEDURES		
	T1.1 Tender Notice and Invitation to Tender	White	2
	T1.2 Tender Data & Evaluation Criteria	Pink	3 – 11
PART T2	RETURNABLE DOCUMENTS		
	T2.1 List of Returnable and Compulsory Documents	Yellow	12 - 20
	T2.2 Returnable Schedules	Yellow	21 - 75
	THE CONTRACT		
PART C1	CONTRACT DATA		
	C1.1 Form of Offer and Acceptance	Yellow	77 – 82
	C1.2.1 General Conditions of Contract	Yellow	83
	C1.2.2 Special Conditions of Contract	Yellow	84– 86
	C1.2.3 Principal Building Agreement Contract Data	Yellow	87 – 119
PART C2	PRICING DATA		
	C2.1 Pricing Instructions	Yellow	69– 71
	C2.2 Bill of Quantities	Yellow	120-131
PART C3	SCOPE OF WORK		
	C3.1 Scope of Works	Blue	132 – 143
	C3.2 Standard Specifications	Blue	144 - 247
PART C4	SITE INFORMATION		
	C4.1 Site Information	Green	248 - 249
	ANNEXURES		
ANNEXURE A	Occupational Health and Safety Specification		
ANNEXURE B	Tender Drawings		

PART T1: TENDERING PROCEDURES

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T1.1 TENDER NOTICE AND INVITATION TO TENDER

Rainprop RF (Pty) Ltd as the Concessionaire hereby invites Tenderers, to tender for:

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)

Security companies must be registered with the Private Security Industry Regulatory Authority (PSiRA) and comply with the Private Security Industry Regulation Act 56 of 2001 to operate legally. These type of companies are hereby invited.

The tender documents are available from:

<https://rainprop.co.za/procurement-suppliers/>

Queries relating to the issue of these documents shall be addressed to the Employer's Agent(s):

Representative to whom Procurement Enquiries must be addressed	Name: Sisonke Ngqasa Email address: sisonke@rainprop.co.za (All enquires must be in writing.)
Representative to whom Technical Enquiries must be addressed	Name: Khaya Ncwana Email address: khaya@rainprop.co.za (All enquires must be in writing.)

A compulsory clarification meeting with representatives of the Employer will take place at:

Place: Rainprop Boardroom

Date: 15 January 2026

Time: 10h00am

The closing venue and time for receipt of tenders is:

Place: Rainprop Tender Box, Block B, DTIC Campus

Date: 29th January 2026

Time: 11h00am

Telegraphic, telephonic, telex, facsimile, e-mail and late tenders will not be accepted.

Type text here

Tenders must only be submitted on the tender documentation that is issued. Requirements for sealing, addressing, delivery, opening and assessment of tenders are stated in the Tender Data.

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T1.2 TENDER DATA & EVALUATION CRITERIA

The conditions of tender are the Standard Conditions of Tender as contained in Annex C of the CIDB Standard for Uniformity in Engineering and Construction Works Contracts (August 2019), Department of Public Works Notice 423 of 2019.

[Standard-for-Uniformity-August-2019.pdf \(cidb.org.za\)](https://www.cidb.org.za/Standard-for-Uniformity-August-2019.pdf)

The Tender Data below provides further clarity, amendments and/or additions to the standard conditions of tender. Each item below is cross-referenced to the clause in the standard conditions of tender to which it applies.

CLAUSE NUMBER	TENDER DATA & EVALUATION CRITERIA
C.1	GENERAL
C.1.1	Actions
C.1.1.1	The Employer is the RAINPROP RF (Pty) Ltd
C.1.2	Tender Documents
C.1.2	The Tender Documents issued by the Employer comprise of the documents as listed on the Contents Page. Other documents as referenced in this tender document
C.1.4	Communication and Employer's agent
C.1.4	Tenderers are to refer to T1.1 – Tender Notice and Invitation to Tender, for the contact details to whom queries are to be addressed to.
C.1.5	Cancellation and Re-Invitation of Tenders
C.1.5.4	The Employer reserves the right to: - Not to appoint the tenderer who has submitted the lowest tendered amount. - Award parts of this tender to different Tenderers. - Make no award and to withdraw and/or cancel the tender at its discretion. - Reserves the right not to award to the highest point scorer, subject to financial viability and security vetting objective criteria being complied with.
C.2	TENDERER'S OBLIGATIONS
C.2.1	Eligibility
C2.1	The Employer will only contract with those Tenderers who satisfy the following criteria: - South African Revenue Service (SARS) Tax Compliance Requirements - It is a condition of the Tender that the taxes of the successful Tenderer must be in order with SARS. - The Valid Tax Compliance PIN Certificate must be submitted together with the Tender. Failure to submit the original and valid Tax Compliance PIN Certificate will result in the invalidation of the Tender.

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T1.2 TENDER DATA & EVALUATION CRITERIA (CONTINUED)

CLAUSE NUMBER	TENDER DATA & EVALUATION CRITERIA
C.2.1	Eligibility (Continued)
C2.1	1.2. Tenderers who are not in possession of a Valid Tax Compliance PIN Certificate are required to complete the Letter of Authorisation Form on T2.2 of the Tender document, granting the Employer authority to verify/ validate the Tenderers Tax Compliance Status with SARS. The Tenderer is also required to attach a copy of the Tenderers Tax Compliance Status printed from the online portal. 1.3. Upon evaluation of the Tender, should the Tenderers Tax Compliance Status printed from the online portal, not be in order, this will lead to the invalidation of the Tender. 2. The Tenderer or any of its directors/ shareholders should not be listed on the Register of Tender Defaulters or database of restricted suppliers in terms of the Prevention and Combating of Corrupt Activities Act of 2004 as a person prohibited from doing business with the public sector. 3. The Tenderer has not: 3.1. abused the Employer's Supply Chain Management System; or 3.2. failed to perform on any previous contract and has been given a written notice to this effect. 4. Only those tenderers who are PSIRA registered are eligible to have their tenders evaluated. 5. It is preferred that tenderers are registered with the CIDB, or if not registered are capable of being so or are able to justify grading equivalency without registration. Where a tenderer is not registered with the CIDB, the tenderer is to submit with the tender offer a justification notice stipulating that the tenderer fulfils the CIDB grading equivalency criteria prior to the evaluation of the submission. The tenderer shall be required to stipulate, with verification, that the tenderer meets or exceeds a level 6 CIDB grading, the requirements of which are determined in accordance with the sum tendered, or a value determined in accordance with Regulation 25 (1B) or 25(7A) of the Construction Industry Development Regulations. Fulfilling either of these requirements is mandatory and compliant tenderers would eligible to have their tenders evaluated. 6. Proof of registration on the National Treasury Central Supplier Database (CSD). 7. The Tenderer has fully complied with this request for TENDER and furnished all the information and documents required listed in the tender returnable schedule.
C.2.5	Reference Documents
	Tenderers are advised to obtain their own copies of the following reference documents: • The CIDB Standard for Uniformity in Engineering and Construction Works Contracts (August 2019), Department of Public Works Notice 423 of 2019 • JBCC Contract (JBCC (Joint Building Contracts Committee) Principal Building Agreement – Edition 6.2 – May 2018) • Other documents deemed necessary that are referenced in this tender document

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T1.2 TENDER DATA & EVALUATION CRITERIA (CONTINUED)

CLAUSE NUMBER	TENDER DATA & EVALUATION CRITERIA
C.2.6	Acknowledge Addenda
C.2.6	Tenderers are to acknowledge receipt of any addenda in the method stated on the addenda
C.2.7	Clarification meeting
	A compulsory clarification meeting with representatives of the Employer will take place at: Place: Rainprop Boardroom Date: 15 th January 2026 Time: 10h00am
C.2.8	Seek clarification
C.2.8	Request clarification of the tender documents, if necessary, by sending written email notification to the employer at least five (5) working days before the closing time stated in the tender data.
C.2.9	Insurance
C.2.9	Refer to C1.2.3 Principal Building Agreement (Contract Data) B 6.0 Insurances
C.2.11	Alterations to Documents
C.2.11	Tenderers shall not make any alterations or additions to the tender documents, except to comply with instructions issued by the employer.
C.2.12	Alternative Tender Offers
C.2.12	No alternative tender offers shall be considered.
C.2.13	Submitting a Tender Offer
C.2.13	- No liability for not specifically mentioning any normal contractual, Common Law or by-law requirements will be accepted by the Employer. - The Tenderer warrants that it has familiarised itself with all the applicable laws and will comply therewith for the purposes of the tender and any agreement which may result therefrom. - Submission of hard copy with electronic copy on a USB. Electronic copy should include the full submission and should also include the Excel BOQ. - The documentation for each Stage of Evaluation shall be submitted separately, in separate envelopes and clearly marked. - Stage 1: Evaluation of Administrative / Mandatory Compliance' - Stage 2: Functionality Evaluation - Stage 3: Evaluation of Price & Preference Point System - Stage 4: Financial Viability Assessment - Stage 5: Security Vetting - All documentation in compliance with the requirements for Stage 1 to 4 should be included in the returnable documents, mandatory submission where stipulated.

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T1.2 TENDER DATA & EVALUATION CRITERIA (CONTINUED)

CLAUSE NUMBER	TENDER DATA & EVALUATION CRITERIA						
	- For the electronic submission; each Stage shall be on a separate folder and clearly marked and populated with the required electronic copy documentation. - Only tenderers that have successfully completed Stage 1 to 4 shall be requested to provide the additional information required for Stage 5 of the evaluation criteria						
C.2.13.5	The Employer's details and address for delivery of tender offers are stated in T1.1 Tender Notice and Invitation to Tender.						
C.2.13.6	A two-envelope system is not applicable (Tenderers to submit their tender with all required documents). Tenders received after the closing time will not be considered.						
C.2.13.7	Identification details The identification details which must be stated in the tender offer outer package are: <table><tr><td>TENDER NUMBER: RFP002-2025/26</td></tr><tr><td>APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26</td></tr><tr><td>CLOSING DATE 29th January 2026</td></tr><tr><td>CLOSING TIME: 11:00 AM</td></tr><tr><td>TENDERER'S NAME:</td></tr><tr><td>TENDERER'S ADDRESS:</td></tr></table>	TENDER NUMBER: RFP002-2025/26	APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26	CLOSING DATE 29th January 2026	CLOSING TIME: 11:00 AM	TENDERER'S NAME:	TENDERER'S ADDRESS:
TENDER NUMBER: RFP002-2025/26							
APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26							
CLOSING DATE 29th January 2026							
CLOSING TIME: 11:00 AM							
TENDERER'S NAME:							
TENDERER'S ADDRESS:							
C.2.13.9	Facsimile, Emailed or Postal Tenders will not be considered. The Employer will not be liable for any costs incurred in the preparation of the tender. Where a tender has been informed per email message of the acceptance of his tender, the acknowledgment of receipt transmitted by his email shall be regarded as proof of delivery to the Tenderer						
C.2.15	Closing Time						
C.2.15.1	The closing time for submission of tender offers is as stated in T1.1 Tender Notice and Invitation to Tender.						
C.2.16	Tender Offer Validity						
C.2.16.1	The tender offer validity period is 120 Calendar Days from the closing date.						
C.2.23	Certificates						
C.2.23	The Tenderer is required to submit with his tender: 1. A Valid Tax Compliance PIN Certificate issued by the South African Revenue Services. 1.1. Tenderers are required to complete the Letter of Authorisation Form on T2.2 of the Tender document, granting the Employer authority to verify/ validate the Tenderers Tax						

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T1.2 TENDER DATA & EVALUATION CRITERIA (CONTINUED)

CLAUSE NUMBER	TENDER DATA & EVALUATION CRITERIA
	Compliance Status with SARS. The Tenderer is also required to attach a copy of the Tenderers Tax Compliance Status printed from the online portal. 1.2. Upon evaluation of the Tender, should the Tenderers Tax Compliance Status printed from the online portal, not be in order, this will lead to the invalidation of the Tender. 2. SBD1 – Invitation to Tender (Closed Tender) 3. SBD4 – Declaration of Interest 4. Proof of good standing in terms of the COID Act 5. B-BBEE Status Level Certificate 6. Proof of good standing in terms of the Unemployment Insurance Fund 7. Proof of registration on the National Treasury Central Supplier Database (CSD) (Mandatory) 8. Company must be registered with Private Security Industry Regulatory Authority (PSIRA) 9. Bank rating letter, will be evaluated in stage 4
C.3	THE EMPLOYER'S UNDERTAKINGS
C.3.4	Opening of Tender Submissions
C.3.4.1	Tenders shall be opened immediately after the closing time for tenders as stipulated in T1.1 Tender Notice and Invitation to Tender. The venue of the Tender opening shall be at Rainprop offices.
C.3.8	Test for Responsiveness
C.3.8	Submission of all documents listed as compulsory in the Returnable Schedule, item T2.1
C.3.11	Evaluation of Tender Offers
C.3.11	The Employer shall apply a five (5) stage process in the evaluation tenders received, namely: Stage 1: Evaluation of Administrative / Mandatory Compliance' Stage 2: Functionality Evaluation Stage 3: Evaluation of Price & Preference Point System Stage 4: Financial Viability Assessment Stage 5: Security Vetting

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T1.2 TENDER DATA & EVALUATION CRITERIA (CONTINUED)

CLAUSE NUMBER	TENDER DATA & EVALUATION CRITERIA																								
C.3.11	Evaluation of Tender Offers																								
C.3.11	<u>STAGE 1: EVALUATION OF ADMINISTRATIVE COMPLIANCE</u>																								
	All tenders received shall be evaluated for Administrative / Mandatory Compliance in terms of the tender requirements & conditions and returnable documents required for evaluation as set out in the returnable schedule in T2.1 of the tender document.																								
	Tenderers are required to complete all forms and submit all information required for the evaluation.																								
	Should the tenderer fail to submit the required information or submit incomplete information after been given a reasonable time to do so, upon request from the bid evaluation committee, and if the information submitted is found to be non-compliant, this would render the tender non-responsive and the tender would be eliminated and not be evaluated any further.																								
	Only tenderers that have provided all the Administrative Documents shall be considered for STAGE 2 evaluation.																								
	<u>STAGE 2: FUNCTIONALITY:</u>																								
	Tenderers are required to submit all information required for the functionality evaluation. If the tenderer fails to submit the required functionality information, this will render the tender non-responsive and the tender would be eliminated and not be evaluated any further under stage 3.																								
	The assessment of functionality will be done in terms of the evaluation criteria and minimum threshold.																								
	A tender will be disqualified if it fails to meet the minimum threshold for functionality.																								
	The minimum Threshold for Functionality applicable to this tender is 70 points, tenderers failing to achieve these points will render the tender non-responsive and the tender would be eliminated and not be evaluated any further for STAGE 3 evaluation.																								
The evaluation criteria and maximum score in respect of each of the criteria are as follows:																									
	<table><tr><th>Doc. Ref.</th><th>Functionality Criteria</th><th>Max. Number of Points</th></tr><tr><td></td><td>Tenderer's Experience</td><td>25</td></tr><tr><td></td><td>Key Staff</td><td>25</td></tr><tr><td></td><td>Health and Safety</td><td>10</td></tr><tr><td></td><td>Programme</td><td>15</td></tr><tr><td></td><td>Methodology</td><td>15</td></tr><tr><td></td><td>OEM Certification</td><td>10</td></tr><tr><td colspan="2">TOTAL:</td><td>100</td></tr></table>	Doc. Ref.	Functionality Criteria	Max. Number of Points		Tenderer's Experience	25		Key Staff	25		Health and Safety	10		Programme	15		Methodology	15		OEM Certification	10	TOTAL:		100
Doc. Ref.	Functionality Criteria	Max. Number of Points																							
	Tenderer's Experience	25																							
	Key Staff	25																							
	Health and Safety	10																							
	Programme	15																							
	Methodology	15																							
	OEM Certification	10																							
TOTAL:		100																							
	Total Points for Functionality: 100 points.																								
	Tenderers able to score a minimum of 70 points or more shall be considered for Stage 3 Evaluation																								

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T1.2 TENDER DATA & EVALUATION CRITERIA (CONTINUED)

CLAUSE NUMBER	TENDER DATA & EVALUATION CRITERIA												
C.3.11	The highest point scorer will be subjected to a functionality viability assessment which is regarded as an objective criterion that Rainprop elects to use for not awarding to the highest point scorer. If the highest points scorer is not functionally viable then the second highest point scorer will be assessed for functionality viability and recommended if they are viable, the process will continue until a functionally viable Tenderer is found, subject to the tendered functionality proposal being competitive, qualitative and market related. 1. Tenderer's Experience Demonstrate a proven capacity and capability to complete works of similar nature. Bidders must ensure that the requested documents are valid as they will be verified. Bidders who submit fraudulent documents will be reported to PSIRA. <table><tr><th>Description</th><th>Points</th><th>Maximum Points</th></tr><tr><td>5 or more INTEGRATED SECURITY SYSTEMS projects with the submission of the following: - Signed Appointment Letter AND - Signed Completion Certificates / Take Over Certificate OR - Signed Final Account Acceptance, with a minimum value of R4.5 million or above per project. Each letter dated 01 January 2018 or later.</td><td>25</td><td>25</td></tr><tr><td>4 or more INTEGRATED SECURITY SYSTEMS projects with the submission of the following: - Signed Appointment Letter AND - Signed Completion Certificates / Take Over Certificate OR - Signed Final Account Acceptance, with a minimum value of R4.5 million or above per project. Each letter dated 01 January 2018 or later .</td><td>20</td><td></td></tr><tr><td>3 or more INTEGRATED SECURITY SYSTEMS projects with the submission of the following: - Signed Appointment Letter AND - Signed Completion Certificates / Take Over Certificate OR - Signed Final Account Acceptance, with a minimum value of R4.5 million or above per project. Each letter dated 01 January 2018 or later .</td><td>15</td><td></td></tr></table>	Description	Points	Maximum Points	5 or more INTEGRATED SECURITY SYSTEMS projects with the submission of the following: - Signed Appointment Letter AND - Signed Completion Certificates / Take Over Certificate OR - Signed Final Account Acceptance, with a minimum value of R4.5 million or above per project. Each letter dated 01 January 2018 or later.	25	25	4 or more INTEGRATED SECURITY SYSTEMS projects with the submission of the following: - Signed Appointment Letter AND - Signed Completion Certificates / Take Over Certificate OR - Signed Final Account Acceptance, with a minimum value of R4.5 million or above per project. Each letter dated 01 January 2018 or later .	20		3 or more INTEGRATED SECURITY SYSTEMS projects with the submission of the following: - Signed Appointment Letter AND - Signed Completion Certificates / Take Over Certificate OR - Signed Final Account Acceptance, with a minimum value of R4.5 million or above per project. Each letter dated 01 January 2018 or later .	15	
Description	Points	Maximum Points											
5 or more INTEGRATED SECURITY SYSTEMS projects with the submission of the following: - Signed Appointment Letter AND - Signed Completion Certificates / Take Over Certificate OR - Signed Final Account Acceptance, with a minimum value of R4.5 million or above per project. Each letter dated 01 January 2018 or later.	25	25											
4 or more INTEGRATED SECURITY SYSTEMS projects with the submission of the following: - Signed Appointment Letter AND - Signed Completion Certificates / Take Over Certificate OR - Signed Final Account Acceptance, with a minimum value of R4.5 million or above per project. Each letter dated 01 January 2018 or later .	20												
3 or more INTEGRATED SECURITY SYSTEMS projects with the submission of the following: - Signed Appointment Letter AND - Signed Completion Certificates / Take Over Certificate OR - Signed Final Account Acceptance, with a minimum value of R4.5 million or above per project. Each letter dated 01 January 2018 or later .	15												

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T1.2 TENDER DATA & EVALUATION CRITERIA (CONTINUED)

CLAUSE NUMBER	TENDER DATA & EVALUATION CRITERIA		
C.3.11	2 or more INTEGRATED SECURITY SYSTEMS projects with the submission of the following: - Signed Appointment Letter AND - Signed Completion Certificates / Take Over Certificate OR - Signed Final Account Acceptance, with a minimum value of R4.5 million or above per project. Each letter dated 01 January 2018 or later .	10	
	1 or more INTEGRATED SECURITY SYSTEMS projects with the submission of the following: - Signed Appointment Letter AND - Signed Completion Certificates / Take Over Certificate OR - Signed Final Account Acceptance, with a minimum value of R4.5 million or above per project. Each letter dated 01 January 2018 or later .	5	
	The tenderer / bidder failed to demonstrate a proven capacity and capability to complete works of similar nature.	0	
	Note: Submission of completion certificate without corresponding appointment letter or submission of appointment letter without corresponding completion certificate will not be considered for scoring purposes. Points will be forfeited.		

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T1.2 TENDER DATA & EVALUATION CRITERIA (CONTINUED)

CLAUSE NUMBER	TENDER DATA & EVALUATION CRITERIA																																						
C.3.11	2. <u>Key Personnel</u>																																						
	<u>Assigned Key Personnel as follows:</u>																																						
	<table><tr><td>Personnel / Criteria</td><td>Points</td><td>Maximum number of Points</td></tr><tr><td colspan="2">Project Lead Electrical / Electronic Engineer</td><td>9</td></tr><tr><td>Qualification</td><td></td><td></td></tr><tr><td>BSC Eng/ B Eng/ BTech</td><td>2</td><td></td></tr><tr><td>National Diploma</td><td>1</td><td></td></tr><tr><td>No Qualification</td><td>0</td><td></td></tr><tr><td>Experience</td><td></td><td></td></tr><tr><td>10+ years Post Qualification</td><td>7</td><td></td></tr><tr><td>8-9 years Post Qualification</td><td>5</td><td></td></tr><tr><td>6-7 years Post Qualification</td><td>3</td><td></td></tr><tr><td>3-5 years Post Qualification</td><td>1</td><td></td></tr><tr><td>1-2 years Post Qualification</td><td>0</td><td></td></tr></table>			Personnel / Criteria	Points	Maximum number of Points	Project Lead Electrical / Electronic Engineer		9	Qualification			BSC Eng/ B Eng/ BTech	2		National Diploma	1		No Qualification	0		Experience			10+ years Post Qualification	7		8-9 years Post Qualification	5		6-7 years Post Qualification	3		3-5 years Post Qualification	1		1-2 years Post Qualification	0	
	Personnel / Criteria	Points	Maximum number of Points																																				
	Project Lead Electrical / Electronic Engineer		9																																				
	Qualification																																						
	BSC Eng/ B Eng/ BTech	2																																					
	National Diploma	1																																					
	No Qualification	0																																					
	Experience																																						
	10+ years Post Qualification	7																																					
	8-9 years Post Qualification	5																																					
	6-7 years Post Qualification	3																																					
	3-5 years Post Qualification	1																																					
	1-2 years Post Qualification	0																																					
	<table><tr><td>Personnel / Criteria</td><td>Points</td><td>Maximum number of Points</td></tr><tr><td colspan="2">Full time Site Agent</td><td>6</td></tr><tr><td>Qualification</td><td></td><td></td></tr><tr><td>BSC Eng/ Beng/ BTech</td><td>2</td><td></td></tr><tr><td>National Diploma</td><td>1</td><td></td></tr><tr><td>No Qualification</td><td>0</td><td></td></tr><tr><td>Experience</td><td></td><td></td></tr><tr><td>10+ years Post Qualification</td><td>4</td><td></td></tr><tr><td>8-9 years Post Qualification</td><td>3</td><td></td></tr><tr><td>6-7 years Post Qualification</td><td>2</td><td></td></tr><tr><td>3-5 years Post Qualification</td><td>1</td><td></td></tr><tr><td>1-2 years Post Qualification</td><td>0</td><td></td></tr></table>			Personnel / Criteria	Points	Maximum number of Points	Full time Site Agent		6	Qualification			BSC Eng/ Beng/ BTech	2		National Diploma	1		No Qualification	0		Experience			10+ years Post Qualification	4		8-9 years Post Qualification	3		6-7 years Post Qualification	2		3-5 years Post Qualification	1		1-2 years Post Qualification	0	
	Personnel / Criteria	Points	Maximum number of Points																																				
	Full time Site Agent		6																																				
	Qualification																																						
	BSC Eng/ Beng/ BTech	2																																					
	National Diploma	1																																					
	No Qualification	0																																					
	Experience																																						
	10+ years Post Qualification	4																																					
	8-9 years Post Qualification	3																																					
	6-7 years Post Qualification	2																																					
	3-5 years Post Qualification	1																																					
	1-2 years Post Qualification	0																																					
	<table><tr><td>Personnel / Criteria</td><td>Points</td><td>Maximum number of Points</td></tr><tr><td colspan="2">QA Personnel</td><td>5</td></tr><tr><td>Qualification</td><td></td><td></td></tr><tr><td>National Diploma</td><td>2</td><td></td></tr><tr><td>No Qualification</td><td>0</td><td></td></tr><tr><td>Experience</td><td></td><td></td></tr><tr><td>8+ years Post Qualification</td><td>3</td><td></td></tr><tr><td>6-7 years Post Qualification</td><td>2</td><td></td></tr><tr><td>3-5 years Post Qualification</td><td>1</td><td></td></tr><tr><td>1-2 years Post Qualification</td><td>0</td><td></td></tr></table>			Personnel / Criteria	Points	Maximum number of Points	QA Personnel		5	Qualification			National Diploma	2		No Qualification	0		Experience			8+ years Post Qualification	3		6-7 years Post Qualification	2		3-5 years Post Qualification	1		1-2 years Post Qualification	0							
	Personnel / Criteria	Points	Maximum number of Points																																				
	QA Personnel		5																																				
	Qualification																																						
	National Diploma	2																																					
No Qualification	0																																						
Experience																																							
8+ years Post Qualification	3																																						
6-7 years Post Qualification	2																																						
3-5 years Post Qualification	1																																						
1-2 years Post Qualification	0																																						

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T1.2 TENDER DATA & EVALUATION CRITERIA (CONTINUED)

CLAUSE NUMBER	TENDER DATA & EVALUATION CRITERIA																																
C.3.11	<table><tr><th>Personnel / Criteria</th><th>Points</th><th>Maximum number of Points</th></tr><tr><td colspan="2">Health & Safety Officer</td><td>5</td></tr><tr><td>Registration</td><td></td><td></td></tr><tr><td>SACPCMP registration</td><td>2</td><td></td></tr><tr><td>No Registration</td><td>0</td><td></td></tr><tr><td>Experience</td><td></td><td></td></tr><tr><td>8+ years Post Qualification</td><td>3</td><td></td></tr><tr><td>6-7 years Post Qualification</td><td>2</td><td></td></tr><tr><td>3-5 years Post Qualification</td><td>1</td><td></td></tr><tr><td>1-2 years Post Qualification</td><td>0</td><td></td></tr></table>			Personnel / Criteria	Points	Maximum number of Points	Health & Safety Officer		5	Registration			SACPCMP registration	2		No Registration	0		Experience			8+ years Post Qualification	3		6-7 years Post Qualification	2		3-5 years Post Qualification	1		1-2 years Post Qualification	0	
	Personnel / Criteria	Points	Maximum number of Points																														
	Health & Safety Officer		5																														
	Registration																																
	SACPCMP registration	2																															
	No Registration	0																															
	Experience																																
	8+ years Post Qualification	3																															
	6-7 years Post Qualification	2																															
	3-5 years Post Qualification	1																															
	1-2 years Post Qualification	0																															
Note: - Failure to submit all the key staff will lead to disqualification - Candidate registrations will not be considered for evaluation																																	
3. <u>Health and Safety</u>																																	
<table><tr><th>Criteria</th><th>Points</th><th>Maximum number of Points</th></tr><tr><td colspan="2">Health & Safety</td><td>10</td></tr><tr><td>1. Policy, organization and management involvement</td><td rowspan="3">2</td><td rowspan="3"></td></tr><tr><td> • Provide a copy of company SHE Policy? </td></tr><tr><td> • Provide company organogram indicating all legal appointments that will be made if successful? </td></tr><tr><td> • Provide proof of registration and good standing with the Compensation Fund or licensed insurer as contemplated in Compensation for Occupational Injuries and Diseases Act (COIDA) </td><td></td><td></td></tr><tr><td>2. Training</td><td rowspan="2">2</td><td rowspan="2"></td></tr><tr><td>Provide proof of health and safety related training provided such as training analysis, Certificates, Job Specific Training or Induction Training program?</td></tr><tr><td>3. Health and Safety Plan</td><td rowspan="2">2</td><td rowspan="2"></td></tr><tr><td> • Provide a project specific health and safety plan . ○ Health and safety plan to include the following minimum criteria? ○ Define health and safety responsibilities for different ○ levels of employees i.e management, supervisors, employees </td></tr></table>			Criteria	Points	Maximum number of Points	Health & Safety		10	1. Policy, organization and management involvement	2		• Provide a copy of company SHE Policy?	• Provide company organogram indicating all legal appointments that will be made if successful?	• Provide proof of registration and good standing with the Compensation Fund or licensed insurer as contemplated in Compensation for Occupational Injuries and Diseases Act (COIDA)			2. Training	2		Provide proof of health and safety related training provided such as training analysis, Certificates, Job Specific Training or Induction Training program?	3. Health and Safety Plan	2		• Provide a project specific health and safety plan . ○ Health and safety plan to include the following minimum criteria? ○ Define health and safety responsibilities for different ○ levels of employees i.e management, supervisors, employees									
Criteria	Points	Maximum number of Points																															
Health & Safety		10																															
1. Policy, organization and management involvement	2																																
• Provide a copy of company SHE Policy?																																	
• Provide company organogram indicating all legal appointments that will be made if successful?																																	
• Provide proof of registration and good standing with the Compensation Fund or licensed insurer as contemplated in Compensation for Occupational Injuries and Diseases Act (COIDA)																																	
2. Training	2																																
Provide proof of health and safety related training provided such as training analysis, Certificates, Job Specific Training or Induction Training program?																																	
3. Health and Safety Plan	2																																
• Provide a project specific health and safety plan . ○ Health and safety plan to include the following minimum criteria? ○ Define health and safety responsibilities for different ○ levels of employees i.e management, supervisors, employees																																	

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T1.2 TENDER DATA & EVALUATION CRITERIA (CONTINUED)

CLAUSE NUMBER	TENDER DATA & EVALUATION CRITERIA		
C.3.11	○ Document health and safety risks and hazards ○ relevant to the project works. ○ Document how health and safety risks and hazards for ○ the contract/project will be identified and mitigated? ○ Document how Safe Working Procedures (SWP/SOP) ○ will be developed and how employees will be trained on such SWP's? ○ Document how health and safety training will be ○ conducted? ○ Document how inspections and audits will be ○ conducted? ○ Document how health and safety communication will ○ be conducted i.e daily safety talks, toolbox talks, incident recalls, safety performance etc ○ Document how health and safety representatives will be appointed and health and safety committees ○ where applicable? ○ Document how occurrences/incidents will be ○ recorded, reported and investigated? ○ Document how Personal Protective Equipment (PPE) ○ will be selected, approved and training of employees on their use? ○ Document how emergency plans will be developed ○ and training of employees on such plans? ○ Fatigue management and Fit for duty processes i.e ○ substance abuse testing and how to deal with positive results, fatigue management addressed?		
	4. Selection, Procurement and Management of Personnel / Subcontractors		
	● Procedure showing how personnel / subcontractors will be assessed to ensure that they are capable of performing the work safely and how they will be managed to ensure compliance to safety requirements?	2	

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T1.2 TENDER DATA & EVALUATION CRITERIA (CONTINUED)

CLAUSE NUMBER	TENDER DATA & EVALUATION CRITERIA																	
C.3.11	5. Fall Protection		2															
	• Provide a fall protection plan to demonstrate that all work at fall risk position will be undertaken under competent supervision, carried out by employees who are trained and medically fit? • Does your fall protection plan include rescue plan, risk assessment, inspection, testing and maintenance of fall protection equipment?																	
	4. Programme																	
	<table><tr><th>Criteria</th><th>Points</th><th>Maximum number of Points</th></tr><tr><td colspan="2">Programme</td><td>15</td></tr><tr><td>Detailed (at least three tier depth – Objectives, tasks, deliverables), project related with critical path and within Contract Period</td><td>15</td><td></td></tr><tr><td>Minimal single tier of main work objectives detail project related and within Contract Period</td><td>8</td><td></td></tr><tr><td>No Submission, or not relevant to Project or beyond Contract Period</td><td>0</td><td></td></tr></table>	Criteria	Points	Maximum number of Points	Programme		15	Detailed (at least three tier depth – Objectives, tasks, deliverables), project related with critical path and within Contract Period	15		Minimal single tier of main work objectives detail project related and within Contract Period	8		No Submission, or not relevant to Project or beyond Contract Period	0			
Criteria	Points	Maximum number of Points																
Programme		15																
Detailed (at least three tier depth – Objectives, tasks, deliverables), project related with critical path and within Contract Period	15																	
Minimal single tier of main work objectives detail project related and within Contract Period	8																	
No Submission, or not relevant to Project or beyond Contract Period	0																	
	5. Methodology																	
	<table><tr><th>Criteria</th><th>Points</th><th>Maximum number of Points</th></tr><tr><td colspan="2">Methodology</td><td>15</td></tr><tr><td>Detailed, project related with risk assessment, quality processes adhered to, deliverables and works within Contract Period</td><td>15</td><td></td></tr><tr><td>Generic with some relevance and within Contract Period (no risk assessment)</td><td>8</td><td></td></tr><tr><td>No Submission, or not relevant to Project</td><td>0</td><td></td></tr></table>	Criteria	Points	Maximum number of Points	Methodology		15	Detailed, project related with risk assessment, quality processes adhered to, deliverables and works within Contract Period	15		Generic with some relevance and within Contract Period (no risk assessment)	8		No Submission, or not relevant to Project	0			
Criteria	Points	Maximum number of Points																
Methodology		15																
Detailed, project related with risk assessment, quality processes adhered to, deliverables and works within Contract Period	15																	
Generic with some relevance and within Contract Period (no risk assessment)	8																	
No Submission, or not relevant to Project	0																	

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T1.2 TENDER DATA & EVALUATION CRITERIA (CONTINUED)

CLAUSE NUMBER	TENDER DATA & EVALUATION CRITERIA																
C.3.11	6. OEM CERTIFICATION The tenderer is to submit certification of having an existing partnership with a reputable OEM as required in the table below. The certification is to confirm that there exists local support through the tenderer of the proposed OEM products and systems to be implemented and that the OEM duly authorises the capability of the tenderer, adequate support to the tenderer and the standing of the tenderer with the OEM. An authorised letter of partnership validation or a copy of a service level agreement or similar validating documentation is to be submitted. <table><tr><th>Criteria</th><th>Points</th><th>Maximum number of Points</th></tr><tr><td colspan="2">ISMS certification</td><td rowspan="6">10</td></tr><tr><td>Proof of relationship with an ISMS OEM</td><td>5</td></tr><tr><td>No proof provided</td><td>0</td></tr><tr><td colspan="2">Gallagher certification</td></tr><tr><td>Proof of relationship with a Gallagher OEM</td><td>5</td></tr><tr><td>No proof provided</td><td>0</td></tr></table> STAGE 3: EVALUATION OF PRICE & PREFERENCE POINT SYSTEM PRICE AND BBBEE - 90/10 PREFERENCE POINT SYSTEM FOR ACQUISITION OF GOODS OR SERVICES WITH RAND VALUE OVER R 70 MILLION All qualifying Tenders that have passed stage 2 of the evaluation process shall be evaluated in terms of Price and preference point system. POINTS AWARDED FOR PRICE The following formula must be used to calculate the points out of 90 for price in respect of a tender with a rand value equal to, or above R 70 000 000(all applicable taxes included): A maximum of 90 points is allocated for price on the following basis: $P_s = 90 \left(1 + \frac{P_t - P_h}{P_h} \right)$ Where P_s = Points scored for price of tender under consideration; P_t = Price of tender under consideration; and P_{min} = Price of lowest acceptable tender. POINTS AWARDED FOR BBBEE STATUS LEVEL OF CONTRIBUTION In terms with the Preferential Procurement Mechanism, preference points will be awarded to a Tenderer for attaining the B-BBEE status level of contribution.	Criteria	Points	Maximum number of Points	ISMS certification		10	Proof of relationship with an ISMS OEM	5	No proof provided	0	Gallagher certification		Proof of relationship with a Gallagher OEM	5	No proof provided	0
Criteria	Points	Maximum number of Points															
ISMS certification		10															
Proof of relationship with an ISMS OEM	5																
No proof provided	0																
Gallagher certification																	
Proof of relationship with a Gallagher OEM	5																
No proof provided	0																

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T1.2 TENDER DATA & EVALUATION CRITERIA (CONTINUED)

CLAUSE NUMBER	TENDER DATA & EVALUATION CRITERIA																				
C.3.11	The following table must be used to calculate the points out of 10 for B-BBEE: <table data-bbox="397 472 1354 1018"> <tr> <th data-bbox="397 472 857 531">B-BBEE STATUS LEVEL OF CONTRIBUTOR</th><th data-bbox="857 472 1354 531">NUMBER OF POINTS</th></tr> <tr> <td data-bbox="397 531 857 583">1</td><td data-bbox="857 531 1354 583">10</td></tr> <tr> <td data-bbox="397 583 857 636">2</td><td data-bbox="857 583 1354 636">9</td></tr> <tr> <td data-bbox="397 636 857 688">3</td><td data-bbox="857 636 1354 688">6</td></tr> <tr> <td data-bbox="397 688 857 741">4</td><td data-bbox="857 688 1354 741">5</td></tr> <tr> <td data-bbox="397 741 857 793">5</td><td data-bbox="857 741 1354 793">4</td></tr> <tr> <td data-bbox="397 793 857 846">6</td><td data-bbox="857 793 1354 846">3</td></tr> <tr> <td data-bbox="397 846 857 898">7</td><td data-bbox="857 846 1354 898">2</td></tr> <tr> <td data-bbox="397 898 857 951">8</td><td data-bbox="857 898 1354 951">1</td></tr> <tr> <td data-bbox="397 951 857 1018">Non-compliant contributor</td><td data-bbox="857 951 1354 1018">0</td></tr> </table> POINTS AWARDED FOR BBBEE STATUS LEVEL OF CONTRIBUTION (CONTINUED) - A tenderer must submit proof of its B-BBEE status level of contributor. Tenderers must submit their valid B-BBEE status level verification certificate or a copy thereof, substantiating their B-BBEE rating issued by a Verification Agency accredited by SANAS. - A trust, consortium or joint venture, will qualify for points for their B-BBEE status level as a legal entity, provided that the entity submits their B-BBEE status level certificate. - A trust, consortium or joint venture will qualify for points for their B-BBEE status level as an unincorporated entity, provided that the entity submits their consolidated B-BBEE scorecard as if they were a group structure and that such a consolidated B-BBEE scorecard is prepared for every separate Tender. - A tenderer failing to submit proof of B-BBEE status level of contribution or is a non-compliant contributor to B-BBEE may not be disqualified, but- - may only score point out of 90 for price; and - scores 0 points out of 10 for Preferential Point System. - A tenderer may not be awarded points for B-BBEE status level of contributor if the tender documents indicate that the tenderer intends subcontracting more than 30% of the value of the contract to any other person not qualifying for at least the points that the tenderer qualifies for, unless the intended subcontractor is an EME that has the capability to execute the subcontract. - Tenderers must submit their original and valid B-BBEE status level verification certificate, substantiating their B-BBEE rating issued by a Registered Auditor approved by IRBA or a Verification Agency accredited by SANAS	B-BBEE STATUS LEVEL OF CONTRIBUTOR	NUMBER OF POINTS	1	10	2	9	3	6	4	5	5	4	6	3	7	2	8	1	Non-compliant contributor	0
B-BBEE STATUS LEVEL OF CONTRIBUTOR	NUMBER OF POINTS																				
1	10																				
2	9																				
3	6																				
4	5																				
5	4																				
6	3																				
7	2																				
8	1																				
Non-compliant contributor	0																				

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T1.2 TENDER DATA & EVALUATION CRITERIA (CONTINUED)

CLAUSE NUMBER	TENDER DATA & EVALUATION CRITERIA
C.3.11	ADJUDICATION USING POINT SYSTEM - The points scored by a tenderer for B-BBEE contribution must be added to the points scored for price. - The Tenderer obtaining the higher number of total points will be assessed for financial viability and security vetting, and will be recommended for award if they are found to be financially viable and successfully security vetted. - Preference points shall be calculated after prices have been brought to a comparative basis taking into account all factors of non-firm prices and all unconditional discounts. - Points scored must be rounded off to the nearest 2 decimals places. - In the event that two or more Tenders have scored equal total points, the successful Tender must be the one scoring the highest number of preference points for Preference Point System. Should two or more Tenders be equal in all respects, the award shall be decided by the drawing of lots. <u>STAGE 4 FINANCIAL VIABILITY</u> The highest point scorer will be subjected a financial viability assessment which is regarded as an objective criteria that Rainprop elects to use for not awarding to the highest point scorer. If the highest points scorer is not financially viable then the second highest point scorer will be assessed for financial viability and recommended if they are financially viable, the process will continue until a financially viable Tenderer is found, subject to the tendered amount and proposal being competitive, qualitative and market related. Tenderers must attach three sets for Audited Annual Financial Statements for three previous financial years with the current ratio calculated. The Annual Financial Statements must include Statement of Financial Position (Balance sheet), Statement of Financial Performance (Income Statement) and Cash Flow Statement. Tenderers will be considered financially viable if they have: - Current ratio is 1:1 for all three financial years - Positive bank balance with a Cash flow balance for the latest financial year must be equal to 15% of the priced contract value by the tenderer. <u>STAGE 5 SECURITY VETTING</u> Tenderers who have successfully completed Stages 01 – Stage 04 will be evaluated for security vetting. Security vetting will only be undertaken on tenderers that have passed all other checks. All employees of the tenderer including and sub contractors are to be Republic of South Africa citizens with appropriate documentation as proof. Tenderers will be required to provide South African identity documents for all personnel intended to work on site at any stage during the contract irrespective of the duration of the personnels' on-site duration.

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T1.2 TENDER DATA & EVALUATION CRITERIA (CONTINUED)

CLAUSE NUMBER	TENDER DATA & EVALUATION CRITERIA
	Security vetting will consist of completion of background checks forms, fingerprints checks, police clearance and / or State Security Agency clearance. (DTIC and Rainprop will assist with documentation for successful tenderer). Should the tenderer (or any individual person) fail to submit the required security vetting information or submit incomplete security vetting information after been given a reasonable time to do so and if the security vetting information submitted is found to be non-compliant, this would render the tender non-responsive and the tender would be eliminated and not be evaluated any further. Should any individual person fail to submit the required security vetting information or submit incomplete security vetting information after been given a reasonable time to do so and if the security vetting information submitted is found to be non-compliant, the person will be denied access to site.
C.3.13	Acceptance of Tender Offer
C.3.13	Tenders will only be accepted if: 1. The Tenderer complies with eligibility criteria as stated in C.2.1 2. The Tenderer has completed all sections of tender document. 3. In instances where any mandatory submission, in a form of Status or Certificates, expires after tender closing or during the evaluation process such Tenderer may be requested to submit valid documentation within fourteen (14) calendar days from the date of request, failing which, the Tenderer will be deemed to be non-responsive.
C.3.17	Provide Copies of the Contracts
C.3.17	The number of paper copies of the signed contract to be provided by the Employer is one .
C.3.18	Provide written reasons for actions taken
C.3.18	Client to publish final results of tender within 120 days of tender closing.

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED
SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA,
SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

PART T2: RETURNABLE DOCUMENTS

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T2.01 LIST OF ALL RETURNABLE & COMPULSORY DOCUMENTS

The Tenderer shall complete and submit the following returnable schedules and documents:

Returnable Schedules

Item	Description	Details	Compulsory (Yes / No) Non-Submission will render to Tenderer non-responsive
Stage 1 – Documents required for Administrative Compliance Evaluation			
T2.02	SBD 1 : Invitation to Tender	Completion of attached forms Where no CIDB Registration or CSR number is available, the tenderer is to submit substantiating letter of CIDB Grading level Compliance	Yes
T2.03	Compulsory Enterprise Questionnaire	Completion of attached forms	Yes
T2.04	SBD 6.1 : Preference Points Claim Form	Completion of attached forms	Yes
T2.05	SBD 2 : Tax Compliance Requirements	Valid tax compliance pin certificate issued by the South Africa Revenue Service in respect of the tenderers Tax Compliance Status with SARS. Failure to submit a VALID Tax Compliance Pin Certificate will result in the invalidation of the Tender. SARS is no longer issues paper-based Tax clearance certificates. Tenderers are required to complete the Letter of Authorisation Form on T2.2 of the Tender document, granting the Employer authority to verify/ validate the Tenderers Tax Compliance Status with SARS. The Tenderer is also required to attach a copy of the Tenderers Tax Compliance Status printed from the online portal. Upon evaluation of the Tender, should the Tenderers Tax Compliance Status printed from the online portal, not be in order, this will lead to the invalidation of the Tender.	Yes
T2.06	Authority for Signatory	Form duly completed and signed	Yes
T2.07	Letter of Good Standing in terms of COIDA Act*	Copy of a letter of Good Standing issued by the Department of Labour, in accordance with the Compensation for Occupational Injuries and Diseases Act (COIDA). –must be valid at the time of close of tender and a valid certificate must be produced at the time of award if the certificate expires between close of tender and award. Upon evaluation of the Tender, should the Tenderers Letter of Good Standing Status printed from the online portal, not be in order, this will lead to the invalidation of the Tender.	Yes

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T2.01 LIST OF ALL RETURNABLE & COMPULSORY DOCUMENTS (CONTINUED)

Item	Description	Details	Compulsory (Yes / No) Non-Submission will render to Tenderer non-responsive
Stage 1 – Documents required for Administrative Compliance Evaluation			
T2.08	CSD registration certificate	National Treasury Central Supplier Database Registration Certificate obtained from National Treasury	Yes
T2.09	Record of Addenda to Tender Documents	Acknowledgement of receipt of addenda	Yes, if applicable
T2.10	Declaration of Correctness of Tender	Form duly completed and signed	Yes
T2.11	Declaration of compliance to specification	Form duly completed and signed	Yes
T2.12	Record of Deviation	Form duly completed and signed	Yes
T2.13	PSIRA Registration	Form duly completed and signed with a certified copy of valid Registration Certificate	Yes
Stage 2 - Documents Required for Functionality			
T2.14	Tenderer's Experience Schedule	As per stage 2 requirements	Yes
T2.15	Experience of Key Personnel	As per stage 2 requirements	Yes
T2.16	Health & Safety Experience	As per stage 2 requirements	Yes
T2.17	Preliminary Programme	As per stage 2 requirements	Yes
T2.18	Construction Methodology	As per stage 2 requirements	Yes
T2.19	OEM Certification	As per stage 2 requirements	Yes
Stage 3 - Documents Required for Evaluation of Price and Preferential Points System			
T2.20	Form of Offer and Acceptance	Completion and Signing of the Form of Offer and Acceptance	Yes
T2.21	Pricing Schedule	Completion of the Pricing Schedule and Summary Page	Yes
Stage 4 – Documents Required for Financial Viability Assessment			
T2.22	3 Years Audited Financial Statements	Financial Statements to include Income Statement, Balance Sheet and Cash Flow Statements.	Yes
Stage 5 – Documents Required for Security Vetting			
T2.23	Security Vetting	Personal details of employees, RSA Identity Documents / permanent residence	

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED
SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA,
SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

STAGE 1 – DOCUMENTS REQUIRED FOR ADMINISTRATIVE COMPLIANCE EVALUATION

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)



the dtic

Department:
 Trade, Industry and Competition
REPUBLIC OF SOUTH AFRICA

T2.02 INVITATION TO BID [SBD 1]

**PART A
 INVITATION TO BID**

YOU ARE HEREBY INVITED TO BID FOR INTEGRATED SECURITY SOLUTION IMPLEMENTATION FOR DTIC CAMPUS					
BID NUMBER:	RAINPROP RFP002-2025/26	CLOSING DATE:	29 January 2026	CLOSING TIME:	11:00 AM
DESCRIPTION	APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)				
BID RESPONSE DOCUMENTS MAY BE DEPOSITED IN THE BID BOX SITUATED AT (STREET ADDRESS)					
RAINPROP (RF) Pty Ltd 77 MEINTJIES STREET, BLOCK B GROUND FLOOR, THE DTIC CAMPUS, SUNNYSIDE, PRETORIA					
BIDDING PROCEDURE ENQUIRIES MAY BE DIRECTED TO:			TECHNICAL INFORMATION MAY BE DIRECTED TO:		
CONTACT PERSON	Sisonke Ngqasa		CONTACT PERSON	Khaya Ncwana	
TELEPHONE NUMBER	012 440 6900		TELEPHONE NUMBER	012 440 6900	
FACSIMILE NUMBER			FACSIMILE NUMBER		
E-MAIL ADDRESS	sisonke@rainprop.co.za		E-MAIL ADDRESS	khaya@rainprop.co.za	
SUPPLIER INFORMATION					
NAME OF TENDERER					
POSTAL ADDRESS					
STREET ADDRESS					
TELEPHONE NUMBER	CODE		NUMBER		
CELLPHONE NUMBER					
FACSIMILE NUMBER	CODE		NUMBER		
E-MAIL ADDRESS					
VAT REGISTRATION NUMBER					

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

SUPPLIER COMPLIANCE STATUS	TAX COMPLIANCE STATUS PIN:		OR	CSD NUMBER:	
----------------------------	----------------------------	--	----	-------------	--

T2.02 INVITATION TO BID CONTINUED [SBD 1]

[A B-BBEE STATUS LEVEL VERIFICATION CERTIFICATE/SWORN AFFIDAVIT (FOR EMEs& QSEs) MUST BE SUBMITTED IN ORDER TO QUALIFY FOR PREFERENCE POINTS FOR B-BBEE]			
ARE YOU THE ACCREDITED REPRESENTATIVE IN SOUTH AFRICA FOR THE GOODS / SERVICES / WORKS OFFERED?	☐ Yes ☐ No [IF YES ENCLOSE PROOF]	ARE YOU A FOREIGN BASED SUPPLIER FOR THE GOODS / SERVICES / WORKS OFFERED?	☐ Yes ☐ No [IF YES ANSWER FOREIGN SUPPLIERS QUESTIONNAIRE BELOW]
QUESTIONNAIRE TO BIDDING FOREIGN SUPPLIERS			
IS THE TENDERER A RESIDENT OF THE REPUBLIC OF SOUTH AFRICA (RSA)?		☐ YES ☐ NO	
DOES THE TENDERER HAVE A BRANCH IN THE RSA?		☐ YES ☐ NO	
DOES THE TENDERER HAVE A PERMANENT ESTABLISHMENT IN THE RSA?		☐ YES ☐ NO	
DOES THE TENDERER HAVE ANY SOURCE OF INCOME IN THE RSA?		☐ YES ☐ NO	
IF THE ANSWER IS "NO" TO ALL OF THE ABOVE, THEN, IT IS NOT A REQUIREMENT TO OBTAIN A TAX COMPLIANCE STATUS / TAX COMPLIANCE SYSTEM PIN CODE FROM THE SOUTH AFRICAN REVENUE SERVICE (SARS) AND IF NOT REGISTER AS PER 2.3 ABOVE.			

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.02 INVITATION TO BID CONTINUED [SBD 1]

SBD1

PART B TERMS AND CONDITIONS FOR BIDDING

1. BID SUBMISSION:
1.1. BIDS MUST BE DELIVERED BY THE STIPULATED TIME TO THE CORRECT ADDRESS. LATE BIDS WILL NOT BE ACCEPTED FOR CONSIDERATION. 1.2. ALL BIDS MUST BE SUBMITTED ON THE OFFICIAL FORMS PROVIDED – (NOT TO BE RE-TYPED) OR IN THE MANNER PRESCRIBED IN THE BID DOCUMENT. 1.3. THIS BID IS SUBJECT TO THE PREFERENTIAL PROCUREMENT POLICY FRAMEWORK ACT, 2000 AND THE PREFERENTIAL PROCUREMENT REGULATIONS, 2022, THE GENERAL CONDITIONS OF CONTRACT (GCC) AND, IF APPLICABLE, ANY OTHER SPECIAL CONDITIONS OF CONTRACT.
2. TAX COMPLIANCE REQUIREMENTS
2.1 TENDERERS MUST ENSURE COMPLIANCE WITH THEIR TAX OBLIGATIONS. 2.2 TENDERERS ARE REQUIRED TO SUBMIT THEIR UNIQUE PERSONAL IDENTIFICATION NUMBER (PIN) ISSUED BY SARS TO ENABLE THE ORGAN OF STATE TO VERIFY THE TAXPAYER'S PROFILE AND TAX STATUS. 2.3 APPLICATION FOR TAX COMPLIANCE STATUS (TCS) PIN MAY BE MADE VIA E-FILING THROUGH THE SARS WEBSITE WWW.SARS.GOV.ZA. 2.4 IN BIDS WHERE CONSORTIA / JOINT VENTURES / SUB-CONTRACTORS ARE INVOLVED, EACH PARTY MUST SUBMIT A SEPARATE TCS CERTIFICATE / PIN / CSD NUMBER. 2.5 WHERE NO TCS PIN IS AVAILABLE BUT THE TENDERER IS REGISTERED ON THE CENTRAL SUPPLIER DATABASE (CSD), A CSD NUMBER MUST BE PROVIDED. 2.6 NO BIDS WILL BE CONSIDERED FROM PERSONS IN THE SERVICE OF THE STATE, COMPANIES WITH DIRECTORS WHO ARE PERSONS IN THE SERVICE OF THE STATE, OR CLOSE CORPORATIONS WITH MEMBERS PERSONS IN THE SERVICE OF THE STATE." 2.7 NO BIDS WILL BE CONSIDERED FROM PERSONS OR COMPANIES LISTED ON THE NATIONAL TREASURY DATABASE OF TENDER DEFAULTERS OR DATABASE OF RESTRICTED SUPPLIERS

NB: FAILURE TO PROVIDE ANY OF THE ABOVE PARTICULARS MAY RENDER THE BID INVALID.

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T2.03 COMPULSORY ENTERPRISE QUESTIONNAIRE [SBD 4]

The following particulars must be furnished. In the case of a joint venture, separate enterprise questionnaires in respect of each partner must be completed and submitted.

Section 1: Name of enterprise:

Section 2: VAT registration number, if any:

Section 3: cidb registration number, if any:

Where there is no registration, a supporting letter to be appended to validate equivalency of compliance to level grading required

Section 4: csd number:

Section 5: Particulars of sole proprietors and partners in partnerships

Name*	Identity number*	Personal income tax number*

** Complete only if sole proprietor or partnership and attach separate page if more than 3 partners*

Section 6: Particulars of companies and close corporations

Company registration number

Close corporation number

Tax reference number

Section 7: The attached SBD 4 must be completed for each tender and be attached as a tender requirement.

Section 8: The attached SBD 6.1 must be completed for each tender and be attached as a requirement.

The undersigned, who warrants that he / she is duly authorised to do so on behalf of the enterprise:

- i) authorizes the Employer to obtain a tax clearance certificate from the South African Revenue Services that my / our tax matters are in order;

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

ii) confirms the neither the name of the enterprise or the name of any partner, manager, director or other person, who wholly or partly exercises, or may exercise, control over the enterprise appears on the Register of Tender Defaulters established in terms of the Prevention and Combating of Corrupt Activities

Act of 2004; iii) confirms that no partner, member, director or other person, who wholly or partly exercises, or may exercise, control over the enterprise appears, has within the last five years been convicted of fraud or corruption;

iv) confirms that I / we are not associated, linked or involved with any other tendering entities submitting tender offers and have no other relationship with any of the tenderers or those responsible for compiling the scope of work that could cause or be interpreted as a conflict of interest; and

iv) confirms that the contents of this questionnaire are within my personal knowledge and are to the best of my belief both true and correct.

Signed

Date

Name

Position

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.04 PREFERENCE POINTS CLAIM FORM [SBD 6.1]

PREFERENCE POINTS CLAIM FORM IN TERMS OF THE PREFERENTIAL PROCUREMENT REGULATIONS 2017

This preference form must form part of all bids invited. It contains general information and serves as a claim form for preference points for Broad-Based Black Economic Empowerment (B-BBEE) Status Level of Contribution

NB: BEFORE COMPLETING THIS FORM, TENDERERS MUST STUDY THE GENERAL CONDITIONS, DEFINITIONS AND DIRECTIVES APPLICABLE IN RESPECT OF B-BBEE, AS PRESCRIBED IN THE PREFERENTIAL PROCUREMENT REGULATIONS, 2017.

1. GENERAL CONDITIONS

1.1 The following preference point systems are applicable to all bids:

- the 80/20 system for requirements with a Rand value of up to R70 000 000 (all applicable taxes included); and
- the 90/10 system for requirements with a Rand value above R70 000 000 (all applicable taxes included).

1.2 The value of this bid is estimated to **exceed** R70 000 000 (all applicable taxes included) and therefore the **90 / 10** preference point system shall be applicable.

1.3 Points for this bid shall be awarded for:

- (a) Price; and
- (b) B-BBEE Status Level of Contributor.

1.4 The maximum points for this bid are allocated as follows:

	POINTS
PRICE	90
B-BBEE STATUS LEVEL OF CONTRIBUTOR	10
Total points for Price and B-BBEE must not exceed	100

1.5 Failure on the part of a Tenderer to submit proof of B-BBEE Status level of contributor together with the bid, will be interpreted to mean that preference points for B-BBEE status level of contribution are not claimed.

1.6 The purchaser reserves the right to require of a Tenderer, either before a bid is adjudicated or at any time subsequently, to substantiate any claim in regard to preferences, in any manner required by the purchaser.

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T2.04 PREFERENCE POINTS CLAIM FORM CONTINUED [SBD 6.1]

2. DEFINITIONS

- (a) **“B-BBEE”** means broad-based black economic empowerment as defined in section 1 of the Broad-Based Black Economic Empowerment Act;
- (b) **“B-BBEE status level of contributor”** means the B-BBEE status of an entity in terms of a code of good practice on black economic empowerment, issued in terms of section 9(1) of the Broad-Based Black Economic Empowerment Act;
- (c) **“bid”** means a written offer in a prescribed or stipulated form in response to an invitation by an organ of state for the provision of goods or services, through price quotations, advertised competitive bidding processes or proposals;
- (d) **“Broad-Based Black Economic Empowerment Act”** means the Broad-Based Black Economic Empowerment Act, 2003 (Act No. 53 of 2003);
- (e) **“EME”** means an Exempted Micro Enterprise in terms of a code of good practice on black economic empowerment issued in terms of section 9 (1) of the Broad-Based Black Economic Empowerment Act;
- (f) **“functionality”** means the ability of a tenderer to provide goods or services in accordance with specifications as set out in the tender documents.
- (g) **“prices”** includes all applicable taxes less all unconditional discounts;
- (h) **“proof of B-BBEE status level of contributor”** means:
 - 1) B-BBEE Status level certificate issued by an authorized body or person;
 - 2) A sworn affidavit as prescribed by the B-BBEE Codes of Good Practice;
 - 3) Any other requirement prescribed in terms of the B-BBEE Act;
- (i) **“QSE”** means a qualifying small business enterprise in terms of a code of good practice on black economic empowerment issued in terms of section 9 (1) of the Broad-Based Black Economic Empowerment Act;
- (j) **“rand value”** means the total estimated value of a contract in Rand, calculated at the time of bid invitation, and includes all applicable taxes;

3. POINTS AWARDED FOR PRICE

3.1 THE 80/20 OR 90/10 PREFERENCE POINT SYSTEMS

A maximum of 80 or 90 points is allocated for price on the following basis:
 80/20 or 90/10

$$P_s = 80 \left(1 - \frac{P_t - P_{\min}}{P_{\min}} \right) \quad \text{or} \quad P_s = 90 \left(1 - \frac{P_t - P_{\min}}{P_{\min}} \right)$$

Where

- P_s = Points scored for price of bid under consideration
- P_t = Price of bid under consideration
- $P_{\min}$ = Price of lowest acceptable bid

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T2.04 PREFERENCE POINTS CLAIM FORM CONTINUED [SBD 6.1]

4. POINTS AWARDED FOR B-BBEE STATUS LEVEL OF CONTRIBUTOR

- 4.1 In terms of Regulation 6 (2) and 7 (2) of the Preferential Procurement Regulations, preference points must be awarded to a Tenderer for attaining the B-BBEE status level of contribution in accordance with the table below:

B-BBEE Status Level of Contributor	Number of points (90/10 system)	Number of points (80/20 system)
1	10	20
2	9	18
3	6	14
4	5	12
5	4	8
6	3	6
7	2	4
8	1	2
Non-compliant contributor	0	0

5. BID DECLARATION

- 5.1 Tenderers who claim points in respect of B-BBEE Status Level of Contribution must complete the following:

6. B-BBEE STATUS LEVEL OF CONTRIBUTOR CLAIMED IN TERMS OF PARAGRAPHS 1.4 AND 4.1

- 6.1 B-BBEE Status Level of Contributor: . =(maximum of 10 or 20 points)
 (Points claimed in respect of paragraph 7.1 must be in accordance with the table reflected in paragraph 4.1 and must be substantiated by relevant proof of B-BBEE status level of contributor.

7. SUB-CONTRACTING

- 7.1 Will any portion of the contract be sub-contracted?

(Tick applicable box)

YES	☐	NO	☐
-----	--------------------------	----	--------------------------

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.04 PREFERENCE POINTS CLAIM FORM CONTINUED [SBD 6.1]

7.1.1 If yes, indicate:

- i) What percentage of the contract will be subcontracted.....%
- ii) The name of the sub-contractor.....
- iii) The B-BBEE status level of the sub-contractor.....
- iv) Whether the sub-contractor is an EME or QSE

(Tick applicable box)

YES		NO	
-----	--	----	--

- v) Specify, by ticking the appropriate box, if subcontracting with an enterprise in terms of Preferential Procurement Regulations, 2017:

Designated Group: An EME or QSE which is at least 51% owned by:	EME √	QSE √
Black people		
Black people who are youth		
Black people who are women		
Black people with disabilities		
Black people living in rural or underdeveloped areas or townships		
Cooperative owned by black people		
Black people who are military veterans		
OR		
Any EME		
Any QSE		

8. DECLARATION WITH REGARD TO COMPANY/FIRM

8.1 Name of company/firm:.....

8.2 VAT registration number:.....

8.3 Company registration number:.....

8.4 TYPE OF COMPANY/ FIRM

- ☐ Partnership/Joint Venture / Consortium
- ☐ One person business/sole propriety
- ☐ Close corporation
- ☐ Company
- ☐ (Pty) Limited

[TICK APPLICABLE BOX]

8.5 DESCRIBE PRINCIPAL BUSINESS ACTIVITIES

.....

.....

.....

.....

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T2.04 PREFERENCE POINTS CLAIM FORM CONTINUED [SBD 6.1]

8.6 COMPANY CLASSIFICATION

- ☐ Manufacturer
☐ Supplier
☐ Professional service provider
☐ Other service providers, e.g. transporter, etc.

[TICK APPLICABLE BOX]

8.7 Total number of years the company/firm has been in business:.....

8.8 I/we, the undersigned, who is / are duly authorised to do so on behalf of the company/firm, certify that the points claimed, based on the B-BBE status level of contributor indicated in paragraphs 1.4 and 6.1 of the foregoing certificate, qualifies the company/ firm for the preference(s) shown and I / we acknowledge that:

- i) The information furnished is true and correct;
- ii) The preference points claimed are in accordance with the General Conditions as indicated in paragraph 1 of this form;
- iii) In the event of a contract being awarded as a result of points claimed as shown in paragraphs 1.4 and 6.1, the contractor may be required to furnish documentary proof to the satisfaction of the purchaser that the claims are correct;
- iv) If the B-BBEE status level of contributor has been claimed or obtained on a fraudulent basis or any of the conditions of contract have not been fulfilled, the purchaser may, in addition to any other remedy it may have –
 - (a) disqualify the person from the bidding process;
 - (b) recover costs, losses or damages it has incurred or suffered as a result of that person's conduct;
 - (c) cancel the contract and claim any damages which it has suffered as a result of having to make less favourable arrangements due to such cancellation;
 - (d) recommend that the Tenderer or contractor, its shareholders and directors, or only the shareholders and directors who acted on a fraudulent basis, be restricted by the National Treasury from obtaining business from any organ of state for a period not exceeding 10 years, after the *audi alteram partem* (hear the other side) rule has been applied; and
 - (e) forward the matter for criminal prosecution.

WITNESSES

1.
2.

.....
 SIGNATURE(S) OF TENDERERS(S)

DATE:

ADDRESS

.....

.....

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.05 TAX COMPLIANCE REQUIREMENTS [SBD 2]

It is a condition of a Tender that the taxes of the successful Tenderer **must** be in order, or that satisfactory arrangements have been made with the South African Revenue Service (SARS) to meet the Tenderer's tax obligations.

1. A Tax Compliance Pin Certificate issued by SARS shall be submitted with the Tender. Failure to submit a **VALID** Tax Compliance Pin Certificate will result in the invalidation of the Tender.
2. SARS no longer issues paper-based Tax clearance certificates. Tenderers are required to complete the **Letter of Authorisation Form** on T2.2 of the Tender document, granting the Employer authority to verify/ validate the Tenderers Tax Compliance Status with SARS. The Tenderer is also required to attach a copy of the Tenderers Tax Compliance Status printed from the online portal.
3. **Upon evaluation of the Tender, should the Tenderers Tax Compliance Status printed from the online portal, not be in order, this will lead to the invalidation of the Tender.**
4. In Tenders where Consortia/ Joint Ventures/ Sub-Service Providers are involved; each party must submit a separate valid Tax Compliance Pin Certificate for their respective organisation.
5. Applications for the Tax Clearance Certificates may also be made via eFiling. In order to use this provision, taxpayers will need to register with SARS as eFilers through the website www.sars.gov.za.
6. Copies of the TCC 001 "Application for a Tax Clearance Certificate" form are available from any SARS branch office nationally or on the website www.sars.gov.za.

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.06 AUTHORITY FOR SIGNATORY

Fill in the relevant portion applicable to the type of organisation

A. COMPANIES

If a Tenderer is a company, a copy of the resolution by the board of directors, personally signed by the chairperson of the board, authorising the person who signs this Tender to do so, as well as to sign any contract resulting from this Tender and any other documents and correspondence in connection with this Tender and/ or contract on behalf of the company must be submitted with this Tender, that is before the closing time and date of the Tender.

AUTHORITY BY BOARD OF DIRECTORS

By resolution passed by the Board of Directors on

_____ 20 _____

Mr/ Mrs _____ (whose signature appears below) has been duly authorised to sign all documents in connection with this Tender on behalf of

(Name of Company) _____

IN HIS/ HER CAPACITY AS: _____

SIGNED ON BEHALF OF COMPANY: _____

(PRINT NAME)

SIGNATURE OF SIGNATORY: _____ **DATE:** _____

WITNESSES: _____

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.06 AUTHORITY FOR SIGNATORY (CONTINUED)

B. SOLE PROPRIETOR (ONE - PERSON BUSINESS)

I, the undersigned _____

Hereby confirm that I am the sole owner of the business trading as

SIGNATURE

DATE

Sole proprietors are required to provide a trade name certificate (file a form) in the city/ province where the business is allocated.

The tenderer is to submit proof of this trading certificate and append to this returnable. This tender may not be considered if the tenderer fails to submit same.

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.06 AUTHORITY FOR SIGNATORY (CONTINUED)

C. PARTNERSHIP

The following particulars in respect of every partner must be furnished and signed by every partner:

Full name of Partner	Residential Address	Signature

We, the partners in the business trading as _____

Hereby authorise _____

To sign this Tender as well as any contract resulting from the Tender and any other documents and correspondence in connection with this Tender and/ or contract on behalf of

Signature	Signature	Signature
Date	Date	Date

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED
SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA,
SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.06 AUTHORITY FOR SIGNATORY (CONTINUED)

D. CLOSE CORPORATION

In the case of a close corporation submitting a Tender, a certified copy of the Founding Statement of such corporation shall be included with the Tender, together with the resolution by its members authorising a member or other official of the corporation to sign the documents on their behalf.

By resolution of members at a meeting on _____ 20_____

at _____

Mr/ Ms _____, whose signature
appears below, has been authorised to sign all documents in connection with this Tender on behalf of (Name of Close
Corporation)

SIGNED ON BEHALF OF CLOSE CORPORATION:

(PRINT NAME) _____

IN HIS/ HER CAPACITY AS _____ **DATE:** _____

SIGNATURE OF SIGNATORY: _____

WITNESSES: 1. _____

2. _____

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.06 AUTHORITY FOR SIGNATORY (CONTINUED)

E. CO-OPERATIVE

A certified copy of the Constitution of the co-operative must be included with the Tender, together with the resolution by its members authoring a member or other official of the co-operative to sign the Tender documents on their behalf.

By resolution of members at a meeting on _____ 20_____

at _____

Mr/ Ms _____, whose signature appears below, has been authorised to sign all documents in connection with this Tender on behalf of (Name of Co-Operative)

SIGNATURE OF AUTHORISED REPRESENTATIVE/ SIGNATORY:

(PRINT NAME) _____

IN HIS/ HER CAPACITY AS _____

DATE: _____

SIGNED ON BEHALF OF CO-OPERATIVE: _____

NAME IN BLOCK LETTERS: _____

WITNESSES: 1. _____

2. _____

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T2.06 AUTHORITY FOR SIGNATORY (CONTINUED)

F. JOINT VENTURES

If a Tenderer is a joint venture, a certified copy of the resolution/ agreement passed/ reached signed by the duly authorised representatives of the enterprises, authorising the representatives who sign this tender to do so, as well as to sign any contract resulting from this tender and any other documents and correspondence in connection with the tender and/ or contract on behalf of the joint venture must be submitted with this tender, before the closing time and date of the tender.

Authority to sign on behalf of the Joint Venture:

By resolution/ agreement passed/ reached by the joint venture partners on _____ 20_____

Mr/ Mrs _____, Mr/ Mrs _____

Mr/ Mrs _____ and Mr/ Mrs _____

(whose signatures appear below) have been duly authorised to sign all documents in connection with this tender on behalf of:

(Name of Joint Venture) _____

In his/ her capacity as: _____

Signed on behalf of (COMPANY NAME): _____
 (PRINT NAME)

Signature _____ Date: _____

In his/ her capacity as: _____

Signed on behalf of (COMPANY NAME): _____
 (PRINT NAME)

Signature _____ Date: _____

In his/ her capacity as: _____

Signed on behalf of (COMPANY NAME): _____
 (PRINT NAME)

Signature _____ Date: _____

In his/ her capacity as: _____

Signed on behalf of (COMPANY NAME): _____
 (PRINT NAME)

Signature _____ Date: _____

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED
SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA,
SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.06 AUTHORITY FOR SIGNATORY (CONTINUED)

G. CONSORTIUM

If a Tenderer is a consortium, a certified copy of the resolution/ agreement passed/ reached signed by the duly authorised representatives of the enterprises, authorising the representatives who sign this tender to do so, as well as to sign any contract resulting from this tender and any other documents and correspondence in connection with the tender and/ or contract on behalf of the consortium must be submitted with this tender, before the closing time and date of the tender.

Authority to sign on behalf of the consortium:

By resolution/ agreement passed/ reached by the consortium partners on _____ 20 _____

Mr/ Mrs _____,

(whose signature appear below) have been duly authorised to sign all documents in connection with this tender on behalf of:

(Name of Consortium) _____

In his/ her capacity as: _____

Signature _____ Date: _____

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.07 LETTER OF GOOD STANDING IN TERMS OF COIDA ACT (COMPENSATION FOR OCCUPATIONAL INJURIES AND DISEASES ACT)

[Letters of good standing to be inserted here]

In Tenders where Consortia/ Joint Ventures/ Sub-Service Providers are involved; each party must submit a separate valid Letter of Good Standing Certificate for their respective organisation.

NOTE: Upon evaluation of the Tender, should the Tenderer/s Letter of Good Standing Status printed from the online portal, not be in order, this will lead to the invalidation of the Tender.

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED
SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA,
SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.08 CSD REGISTRATION REPORT

[National Treasury Central Supplier Database Registration Certificate obtained from National Treasury to be inserted here]

In Tenders where Consortia/ Joint Ventures/ Sub-Service Providers are involved; each party must submit a separate copy of CSD Certificate for their respective organisation.

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.09 RECORD OF ADDENDA TO TENDER DOCUMENTS

I/ We confirm that the following communications amending the Tender documents that I/ we received from the Employer or its representative before the closing date for submission of Tenders have been taken into account in this Tender.

A signed copy of each addendum shall be inserted after this page.

ADDENDUM NO.	DATE	TITLE OR DETAILS

Signature
 (of person authorised to sign on behalf of the Tenderer)

Date

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED
SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA,
SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.10 DECLARATION OF CORRECTNESS OF TENDER

I, _____ (Full Name) the Authorised Signatory of

_____ (Tenderer) hereby declare that the information furnished in

the tender is entirely true and correct; and the tender is submitted on condition that the Tenderer; its facilities, etc., shall at any stage be subject to inspection.

SIGNATURE: _____ **DATE:** _____
(of person authorised to sign on behalf of the Tenderer)

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.11 DECLARATION OF COMPLIANCE TO SPECIFICATION

STATEMENT OF COMPLIANCE OR/ OF QUALIFICATIONS BY TENDERER

This Tender complies in every respect with the Technical Specification, Schedules and Drawings –

* (Indicate which is not applicable)

YES	
NOI	

If (NO). detail qualifications hereunder. Failure to detail qualifications shall signify compliance.

QUALIFICATIONS		
PART NO	CLAUSE NO	QUALIFICATIONS

DATE: _____

SIGNATURE OF TENDERER

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.12 RECORD OF DEVIATION

Tenderers to list items that are a variation to the bill of quantities and drawings

ITEM	DESCRIPTION	UNIT	QUANTITY	TARIFF	RANDS	CENTS
	Variation to bill items requested.					

DATE: _____

SIGNATURE OF TENDERER

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.13 PSIRA REGISTRATION CERTIFICATE

[PSIRA Registration Certificate obtained from Private Security Industry Regulatory Authority to be inserted here]

In Tenders where Consortia/ Joint Ventures/ Sub-Service Providers are involved; each party must submit a separate copy of PSIRA Certificate for their respective organisation.

All Certificates to be valid at the time of submission.

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED
SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA,
SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

STAGE 2 – DOCUMENTS REQUIRED FOR FUNCTIONALITY ASSESSMENT

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.14 TENDERER'S EXPERIENCE SCHEDULE

The experience of the tendering entity as opposed to the key staff members/ experts, in projects of SIMILAR TYPE AND SCALE (i.e., Similar Experience) over the last ten years, will be evaluated.

Contact details of clients of the relevant projects must also be provided.

The tenderer is to submit verifiable client reference sheets, i.e., Reference Letter on a Client's Letter Head confirming satisfactory performance, Appointment Letter, and Practical Completion Certificate (Signed by the Principal Agent/ Project Manager/ Authorized Company Representative) - failing which, zero points will be awarded.

The tenderer should populate the attached "Tenderers Experience Schedule T2.2.13" for bid evaluation administrative purposes only.

Tenderers are to have a demonstrable record of working with/on INTEGRATED SECURITY SYSTEMS of a similar value and level of complexity to that of the work described in this tender. SIMILAR EXPERIENCE is defined as having experience in building projects which should include works related to:

1. Integrated Security Systems
2. Surveillance Systems
3. Access Control

NOTE: ZERO (0) POINTS SHALL BE AWARDED FOR PROJECTS THAT DO NOT COMPLY WITH DEFINITION OF SIMILAR EXPERIENCE AS DESCRIBED ABOVE.

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T2.2.13 TENDERER'S EXPERIENCE SCHEDULE (CONTNUED)

The evaluation and scoring will be as follows:

Description	Points	Maximum Points
5 or more INTEGRATED SECURITY SYSTEMS projects with the submission of the following: - Signed Appointment Letter AND - Signed Completion Certificates / Take Over Certificate OR - Signed Final Account Acceptance, with a minimum value of R4.5 million or above per project. Each letter dated 01 January 2018 or later.	25	25
4 or more INTEGRATED SECURITY SYSTEMS projects with the submission of the following: - Signed Appointment Letter AND - Signed Completion Certificates / Take Over Certificate OR - Signed Final Account Acceptance, with a minimum value of R4.5 million or above per project. Each letter dated 01 January 2018 or later.	20	
3 or more INTEGRATED SECURITY SYSTEMS projects with the submission of the following: - Signed Appointment Letter AND - Signed Completion Certificates / Take Over Certificate OR - Signed Final Account Acceptance, with a minimum value of R4.5 million or above per project. Each letter dated 01 January 2018 or later.	15	
2 or more INTEGRATED SECURITY SYSTEMS projects with the submission of the following: - Signed Appointment Letter AND - Signed Completion Certificates / Take Over Certificate OR - Signed Final Account Acceptance, with a minimum value of R4.5 million or above per project. Each letter dated 01 January 2018 or later.	10	
1 or more INTEGRATED SECURITY SYSTEMS projects with the submission of the following: Signed Appointment Letter AND	5	

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

Description	Points	Maximum Points
- Signed Completion Certificates / Take Over Certificate OR - Signed Final Account Acceptance, with a minimum value of R4.5 million or above per project. Each letter dated 01 January 2018 or later.		
The tenderer / bidder failed to demonstrate a proven capacity and capability to complete works of similar nature.	0	
Note: Submission of completion certificate without corresponding appointment letter or submission of appointment letter without corresponding completion certificate will not be considered for scoring purposes. Points will be forfeited.		

Note: in the case of a Joint Venture (JV) at least one member of the JV must submit projects experience within the stipulated range.

Confidential



**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED
FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

**SECURITY SOLUTION AND IMPLEMENTATION
2025/26)**

T2.14 TENDERER'S EXPERIENCE SCHEDULE (CONTINUED)

Schedule A: Similar Experience

To be completed for bid evaluation administrative purposes only.

ITEM	EMPLOYER, CONTACT PERSON AND TELEPHONE NUMBER	DESCRIPTION OF THE PROJECT	DETAILED DESCRIPTION AND DISCIPLINES INVOLVED	VALUE OF PROJECT	PROJECT DURATION	YEAR COMPLETED	PRINCIPAL AGENT, CONTACT PERSON AND TELEPHONE NUMBER
E.g.	RAINPROP Ms A Some 031 xxx xxxx	Ingrated Security at the dtic campus	The scope of the work will encompass Security Systems Integration related to the facilities mentioned above. This includes access control, surveillance and specialized services and works	R6.0m	22 Months	2022	ABC Consulting, Ms A Some 031 xxx xxxx
Projects with a minimum value of R 4 500 000.00				List the most recent projects after 2018 up to a maximum of five (5) projects			
1							
2							
3							
4							
5							

Note: the first five will be evaluated only, projects listed thereafter shall not be evaluated

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T2.15 EXPERIENCE OF KEY PERSONNEL

The experience of assigned staff member/s in relation to the scope of work will be evaluated using the following criteria:

- 1) Submission of an Organogram indicating the following levels of resources as a minimum: Project Manager, Site Agent, Quantity Surveyor, Senior Foreman and Health & Safety Officer. The years of experience in their current position is to be indicated in the Organogram (for administrative purpose only).
- 2) A copy of the relevant certified copies of qualifications are to be submitted, failing which, zero points will be awarded for qualifications.
- 3) The skills and experience of the assigned staff are of similar nature in the operational area which the staff have been resourced.
- 4) Failure to submit CV's or incomplete CV's of the key personnel listed in the scoring below will be scored zero.

Tenderers are required to submit CV's for separate resources. Duplicate resources that are included in more than one position / category will only be evaluated in one position / category. The tenderer will be scored zero points for the resource in the second position / category.

The CVs of the key personnel of not more than 2 pages each should be attached to this schedule. Each CV should be structured as per the template contained within the Tender document located under Section T2.15.

All qualifications issued to be recognised by the South African Qualification Authority (SAQA).

The scoring will be as follows:

Personnel / Criteria	Points	Maximum number of Points
Project Lead Electrical / Electronic Engineer		9
Qualification		
BSC Eng/ B Eng/ BTech	2	
National Diploma	1	
No Qualification	0	
Experience		
10+ years Post Qualification	7	
8-9 years Post Qualification	5	
6-7 years Post Qualification	3	
3-5 years Post Qualification	1	
1-2 years Post Qualification	0	

Personnel / Criteria	Points	Maximum number of Points
Full time Site Agent		6
Qualification		
BSC Eng/ Beng/ BTech	2	
National Diploma	1	
No Qualification	0	

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

Experience		
10+ years Post Qualification	4	
8-9 years Post Qualification	3	
6-7 years Post Qualification	2	
3-5 years Post Qualification	1	
1-2 years Post Qualification	0	

Personnel / Criteria	Points	Maximum number of Points
QA Personnel		5
Qualification		
National Diploma	2	
No Qualification	0	
Experience		
8+ years Post Qualification	3	
6-7 years Post Qualification	2	
3-5 years Post Qualification	1	
1-2 years Post Qualification	0	

Personnel / Criteria	Points	Maximum number of Points
Health & Safety Officer		5
Registration		
SACPCMP registration	2	
No Registration	0	
Experience		
8+ years Post Qualification	3	
6-7 years Post Qualification	2	
3-5 years Post Qualification	1	
1-2 years Post Qualification	0	

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.15 EXPERIENCE OF KEY PERSONNEL (CONTINUED)

Tenderers are required to submit the Key Personnel Schedule as indicated below, If a different format is utilised, bidders are to ensure that the information shown in the template below is provided.

KEY PERSONNEL	NAME	YEARS OF EXPERIENCE	PERIOD WITH COMPANY	HIGHEST VALUE CONTRACT HANDLED
LEAD ENGINEER				
SITE AGENT				
QUALITY ASSURANCE				
HEALTH & SAFETY OFFICER				

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.15 EXPERIENCE OF KEY PERSONNEL (CONTINUED)

Tenderers are required to submit Curriculum vitae (CV) for each of the Key Personnel for which points are awarded. Please note that each CV can only be used for one key personnel position. If a different format is utilised, bidders are to ensure that the information shown in the template below is provided.

CURRICULUM VITAE TEMPLATE OF KEY PERSONNEL									
DESIGNATION.....									
Name:					Date of birth:				
Profession:					Nationality:				
Formal Qualifications:									
Qualification		From: Name of Institution			Year Obtained				
1									
2									
3									
4									
5									
Professional Registrations/ Designation:									
	Professional Registrations/ Designation	Professional Body/Council			Registration Number				
1									
2									
3									
4									
5									
Name of Current Employer (firm):					Full Time:	Yes		No	
Current Position:					Years of Experience:				
Name of Previous Employer (firm):					Full Time:	Yes		No	
Position held:					Years of Experience:				
Name of Previous Employer (firm):					Full Time:	Yes		No	
Position held:					Years of Experience:				

[illegible]

T2.16 TENDERER'S HEALTH & SAFETY EXPERIENCE SCHEDULE

The Safety Plan shall clearly describe the construction activities, risks, methodologies, etc.

The evaluation and scoring will be as follows the Tenderers Health & Safety:

Criteria	Points	Maximum number of Points
Health & Safety		10
6. Policy, organization and management involvement	2	
Provide a copy of company SHE Policy?		
Provide company organogram indicating all legal appointments that will be made if successful?		
Provide proof of registration and good standing with the Compensation Fund or licensed insurer as contemplated in Compensation for Occupational Injuries and Diseases Act (COIDA)		
7. Training	2	
Provide proof of health and safety related training provided such as training analysis, Certificates, Job Specific Training or Induction Training program?		
8. Health and Safety Plan	2	
- Provide a project specific health and safety plan . - Health and safety plan to include the following minimum criteria? - Define health and safety responsibilities for different - levels of employees i.e management, supervisors, employees - Document health and safety risks and hazards - relevant to the project works. - Document how health and safety risks and hazards for - the contract/project will be identified and mitigated? - Document how Safe Working Procedures (SWP/SOP) - will be developed and how employees will be trained on such SWP's? - Document how health and safety training will be - conducted?		

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

Criteria	Points	Maximum number of Points
Health & Safety		10
○ Document how inspections and audits will be conducted? ○ Document how health and safety communication will be conducted i.e daily safety talks, toolbox talks, incident recalls, safety performance etc ○ Document how health and safety representatives will be appointed and health and safety committees where applicable? ○ Document how occurrences/incidents will be recorded, reported and investigated? ○ Document how Personal Protective Equipment (PPE) will be selected, approved and training of employees on their use? ○ Document how emergency plans will be developed and training of employees on such plans? ○ Fatigue management and Fit for duty processes i.e substance abuse testing and how to deal with positive results, fatigue management addressed?		
9. Selection, Procurement and Management of Personnel / Subcontractors		
• Procedure showing how personnel / subcontractors will be assessed to ensure that they are capable of performing the work safely and how they will be managed to ensure compliance to safety requirements?	2	
10. Fall Protection		
• Provide a fall protection plan to demonstrate that all work at fall risk position will be undertaken under competent supervision, carried out by employees who are trained and medically fit? • Does your fall protection plan include rescue plan, risk assessment, inspection, testing and maintenance of fall protection equipment?	2	

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.17 PRELIMINARY PROGRAMME

The Tenderer shall submit a detailed programme clearly decomposing the construction activities by indicating the hierarchy of activities.

The activities shall indicate the duration and the dependencies between the tasks.

The proposed programme showing but not limited to the following:

- Ability to execute the works in terms of the Employer's requirements within the required timeframe indicating the order and timing of the construction that will take place in order to provide the works.
- Taking into account and not limited to start date, access date, completion date, long lead item, and SHE and quality requirements for startup stated in the contract data.

Note: The Contractor must take note of the constraints in the compiling of his construction programme. No other completion time that may be indicated on this programme will be regarded as an alternative offer, all as specified in the Tender Data.

Minimum requirements for the programme:

- Adequate work break-down structure and subtasks aligned to scope of work and services.
- Sequential links
- Key stakeholder approvals / Stage Gates
- Critical path
- Minimum open-ended tasks
- Float
- Baseline
- Risk management
- Testing & Commissioning

In addition to construction activities, the programme is to allow and include for the following:

- Annual builders' holiday
- 15 working days float for project delays such as but not limited to inclement and exceptionally inclement weather.

The overall project duration is **24 Months**.

The successful tenderer will be requested to revise the programme to accommodate the shift in the start date.

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

T2.17 PRELIMINARY PROGRAMME (CONTINUED)

NOTE: Should the tender programme exceed the project duration of 24 months (24 months including provision for project delays), the tenderer shall be scored zero points for this section.

Criteria	Points	Maximum number of Points
Programme		15
Detailed (at least three tier depth – Objectives, tasks, deliverables aligned with methodology), project related with critical path and within Contract Period		15
Adequate detailed work break-down structure and subtasks aligned to scope of work and services.	3	
Sequential links	1	
Key stakeholder approvals / Stage Gates	2	
Critical path	1	
Minimum open-ended tasks	1	
Float	1	
Baseline	1	
Risk management	3	
Testing & Commissioning	2	
Minimal single tier of main work objectives detail project related and within Contract Period	2	2
No Submission, or not relevant to Project or beyond Contract Period	0	0

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.18 CONSTRUCTION METHODOLOGY

The Tenderer is discouraged from producing a generic method statement. The Method Statement must be concise and clearly demonstrate how this project will be implemented.

The Method Statement shall clearly describe the sequencing of the construction activities.

The Tenderer is to describe in detail the responsibilities of key personnel in relation to the construction activities. The Method Statement must also demonstrate what communication and documentation systems are put in place to ensure that the team will be operating at its optimum.

The Method Statement must clearly demonstrate how key components relating to time, risks, cost and quality control will be addressed and managed during all stages of the project life cycle.

Methodology and Work Plan (Including risk allocation and management between design and construction):

- The method statement must respond to the scope of work and outline the proposed approach / methodology. The method statement should articulate what value the Respondent will add in achieving the stated objectives for the project.
- The Respondent must as such explain his / her understanding of the objectives of the assignment and the Employer's stated and implied requirements, highlight the issues of importance, and explain the technical approach they would adopt to address them.
- The approach paper should explain the methodologies which are to be adopted, demonstrate the compatibility of those methodologies with the proposed approach.
- The approach should also include a quality plan which outlines processes, procedures and associated resources, applied by whom and when, to meet the requirements and indicate how risks will be managed and what contribution can be made regarding value management.

The Methodology shall include and address at least the following criteria:

- Project Specific Method Statement and Approach to the Works
- Site Establishment, Approval, De-establishment
- List the plant and equipment and availability dates
- Work Plan
- Asset management (removal, disposal, replacement, allowance for new assets)
- Risk and Responsibilities Allocation
- Management between design and construction
- Programme, etc.
- Commissioning, Compliance, Verification
- Waste removal, disposal
- Integration of SHEQ
- Understanding of the new Construction Regulation 2014

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)

Criteria	Points	Maximum number of Points
Methodology		15
Detailed, project related with risk assessment, quality processes adhered to, deliverables and works within Contract Period		13
Project Specific Method Statement and Approach to the Works	2	
Site Establishment, Approval, De-establishment	1	
List the plant and equipment and availability dates	1	
Work Plan	1	
Asset management (removal, disposal, replacement, allowance for new assets)	1	
Risk and Responsibilities Allocation	2	
Management between design and construction	1	
Commissioning, Compliance, Verification	1	
Waste removal, disposal	1	
Integration of SHEQ	1	
Understanding of the new Construction Regulation 2014	1	
Generic with some relevance and within Contract Period (no risk assessment)	2	2
No Submission, or not relevant to Project	0	0

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.19 OEM CERTIFICATION

The tenderer is to submit certification of having an existing partnership with a reputable OEM as required in the table below. The certification is to confirm that there exists local support through the tenderer of the proposed OEM products and systems to be implemented and that the OEM duly authorises the capability of the tenderer, adequate support to the tenderer and the standing of the tenderer with the OEM. An authorised letter of partnership validation or a copy of a service level agreement or similar validating documentation is to be submitted.

If the Service Provider/tenderer have their own bespoke ISMS, they should submit a letter to that effect, because they will serve as OEM for their product.

Criteria	Points	Maximum number of Points
ISMS certification		10
Proof of relationship with an ISMS OEM	5	
No proof provided	0	
Gallagher certification		
Proof of relationship with a Gallagher OEM	5	
No proof provided	0	

NOTE: For STAGE 2, the minimum Threshold for Functionality applicable to this tender is 70 points, tenderers failing to achieve these points will render the tender non-responsive and the tender would be eliminated and not be evaluated any further.

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED
SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA,
SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

STAGE 3 - DOCUMENTS REQUIRED FOR EVALUATION OF PRICE AND PREFERENTIAL POINTS SYSTEM

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED
SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA,
SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.20 FORM OF OFFER AND ACCEPTANCE

Tenderers are required to complete the Form of Offer and Acceptance and attached same hereunder.

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.21 PRICING SCHEDULE

Tenderers are required to complete the Bill of Quantities / Pricing Schedule and attached same hereunder.

Tenderers are required to complete the Bill of Quantities / Pricing Schedule and attached same hereunder.

GENERAL

The Bill of Quantities forms part of the Contract Documents and must be read and priced in conjunction with all the other documents comprising the Contract Documents, which include the Conditions of Tender, Conditions of Contract, the Specifications (including the Project Specification) and the Drawings.

DESCRIPTION OF ITEMS IN THE SCHEDULE

The short descriptions of the items in the Bill of Quantities are for identification purposes only and the measurement and payment clause of the Standardized Specifications and the Particular Specifications, read together with the relevant clauses of the Project Specification and directives on the drawings, set out what ancillary or associated work and activities are included in the rates for the operations specified.

QUANTITIES REFLECTED IN THE SCHEDULE

The quantities given in the Bill of Quantities are estimates only, and subject to re-measuring during the execution of the work. The Contractor shall obtain the Engineer's detailed instructions for all work before ordering any materials or executing work or making arrangements for it.

The Works as finally completed in accordance with the Contract shall be measured and paid for as specified in the Bill of Quantities and in accordance with the General and Special Conditions of Contract, the Specifications and Project Specifications and the Drawings. Unless otherwise stated, items are measured net in accordance with the Drawings, and no allowance has been made for waste.

The validity of the contract will in no way be affected by differences between the quantities in the Bill of Quantities and the quantities finally certified for payment.

PROVISIONAL SUMS

Where Provisional sums or Prime Cost sums are provided for items in the Bill of Quantities, payment for the work done under such items will be made in accordance with Clause 45 of the General Conditions of Contract 2015. The Employer reserves the right, during the execution of the works, to adjust the stated amounts upwards or downwards according to the work actually done under the item, or the item may be omitted altogether, without affecting the validity of the Contract.

The Tenderer shall not under any circumstances whatsoever delete or amend any of the sums inserted in the "Amount" column of the Bill of Quantities and in the Summary of the Bill of Quantities unless ordered or authorized in writing by the Employer before closure of tenders. Unauthorized changes made by the Tenderer to provisional items in the Bill of Quantities, or to the provisional percentages and sums in the Summary of the Bill of Quantities will lead to the disqualification of the Tenderer.

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

PRICING OF THE BILL OF QUANTITIES

The prices and rates to be inserted by the Tenderer in the Bill of Quantities shall be the full inclusive prices to be paid by the Employer for the work described under the several items, and shall include full compensation for all costs and expenses that may be required in and for the completion and maintenance during the defects liability period of all the work described and as shown on the drawings as well as all overheads, profits, incidentals and the cost of all general risks, liabilities and obligations set forth or implied in the documents on which the Tender is based.

Each item shall be priced and extended to the "Total" column by the Tenderer, with the exception of the items for which only rates are required, or items which already have Prime Cost or Provisional Sums affixed thereto. If the Contractor omits to price any items in the Bill of Quantities, then these items will be considered to have a nil rate or price.

All items for which terminology such as "inclusive" or "not applicable" have been added by the Tenderer will be regarded as having a nil rate which shall be valid irrespective of any change in quantities during the execution of the Contract.

The Tenderer shall fill in rates for all items where the words "rate only" appear in the "Total" column. "Rate Only" items have been included where:

- (a) an alternative item or material is contemplated;
- (b) variations of specified components in the make-up of a pay item may be expected; and
- (c) no work under the item is foreseen at tender stage but the possibility that such work may be required is not excluded.

For "Rate Only" items no quantities are given in the "Quantity" column but the quoted rate shall apply in the event of work under this item being required. The Tenderer shall however note that in terms of the Tender Data the Tenderer may be asked to reconsider any such rates which the Employer may regard as unbalanced.

All rates and amounts quoted in the Bill of Quantities shall be in Rands and cents and shall include all levies and taxes (other than VAT). VAT will be added in the summary of the Bill of Quantities.

"The Contractor shall be deemed to have inspected and examined the Site and its surroundings and information available in connection therewith and to have satisfied himself before submitting his tender (as far as is practicable) as to:

- (a) the form and nature of the Site and its surroundings, including subsurface conditions,
- (b) the hydrological and climatic conditions,
- (c) the extent and nature of work and materials necessary for the execution and completion of the Works,
- (d) the means of access to the Site and the accommodation he may require

and, in general, shall be deemed to have obtained all information (as far as is practicable) as to risks, contingencies and all other circumstances which may influence or affect his Tender"

CORRECTION OF ENTRIES

Incorrect entries shall not be erased or obliterated with correction fluid but must be crossed out neatly. The correct figures must be entered above or adjacent to the deleted entry, and the alteration must be initialled by the Tenderer.

ARITHMETICAL ERRORS

Arithmetical errors found in the Bill of Quantities as a result of faulty multiplication or addition, will be corrected at the tender evaluation stage, in line with the CIDB principles of correcting the arithmetic errors.

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED
SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA,
SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

UNITS OF MEASUREMENT

The units of measurement described in the Bill of Quantities are metric units for which the standard international abbreviations are used. Non-standard abbreviations which may appear in the Bill of Quantities are as follows:

No.	=	Number
%	=	Percent
Sum	=	Lump sum
PC Sum	=	Prime cost sum
Prov sum	=	Provisional sum
m ³ .km	=	Cubic metre - kilometre
Km-pas	=	kilometre - pass
m ² . pass	=	square metre – pass

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

STAGE 4 - FINANCIAL VIABILITY ASSESSMENT

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.22 3 YEARS AUDITED FINANCIAL STATEMENTS

Tenderers are required to provide 3 years of Audited Financial Statements including Income Statement, Balance Sheets and Cash Flow Statements.

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED
SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA,
SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

STAGE 5 – SECURITY VETTING

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
TENDER NO.: RAINPROP RFP No.: RFP002-2025/26)**

T2.23 SECURITY VETTING

Tenderers who have successfully completed Stages 1 – Stage 4 will be evaluated for security vetting. Security vetting will only be undertaken on tenderers that have passed all other checks.

Tenderers are to note that ALL personnel coming onto site will be required to complete background checks, fingerprints checks, police clearance and / or State Security Agency clearance.
(DTIC and Rainprop will facilitate the security vetting process for the successful tenderer)

All employees and specialists appointed under the contractor and his sub contractors are to be RSA citizens / permanent residents with valid South African Identity Document.

All employees of the tenderer intended to work on site including employees of domestic / selected / nominated sub-contractors are to be Republic of South Africa citizens RSA citizens / permanent residents with valid South African Identity Document.

Tenderers will be required to provide documentation for all personnel intended to work on site at any stage during the contract irrespective of the duration of the personnels' on-site duration.

Security vetting will consist of completion of background checks forms, fingerprints checks, police clearance and / or State Security Agency clearance.

Security vetting procedure will consist of the following procedure:

1. The principal agent will collect and submit the following documents from the Tenderer to the dtic VFU:
 - a. Applicant Consent form - signed and dated
 - b. Declaration of Secrecy – signed and dated
 - c. Copy of valid RSA Identification document.
2. An appointment for the Tenderer to come for electronic fingerprints to the VFU.
 - a. Appointments to be at least two weeks before the commencement of the works.
 - b. Appointment to arranged for Mondays and Tuesdays between 09h00 and 12h45. (20 people per day)
3. The VFU will submit the fingerprints to the service provider and the balance of the days of the week would be reasonable sufficient time for the service provider to provide feedback on the fingerprints and the VFU to evaluate the outcome

Should the tenderer (or any individual person) fail to submit the required security vetting information or submit incomplete security vetting information after been given a reasonable time to do so and if the security vetting information submitted is found to be non-compliant, this would render the tender non-responsive and the tender would be eliminated and not be evaluated any further.

Should any individual person fail to submit the required security vetting information or submit incomplete security vetting information after been given a reasonable time to do so and if the security vetting information submitted is found to be non-compliant, the person will be denied access to site.

The tenderer should note that any specialists required for commissioning and verification of equipment will also be subject to the vetting process before they can be allowed onto site.

**APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY
SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA
FROM THE TENDER (RFP002-2025/26)**

PART C1: AGREEMENT AND CONTRACT DATA

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)

C1.1 FORM OF OFFER AND ACCEPTANCE

A. OFFER

The Employer, identified in the Acceptance signature block, has solicited offers to enter into a contract for the procurement of:

TENDER NO RFP002-2025/26.: APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26).

The Tenderer, identified in the Offer signature block, has examined the documents listed in the Tender Data and addenda thereto as listed in the Returnable Schedules, and by submitting this Offer has accepted the Conditions of Tender.

By the representative of the Tenderer, deemed to be duly authorised, signing this part of this Form of Offer and Acceptance, the Tenderer offers to perform all of the obligations and liabilities of the Service Provider under the contract including compliance with all its terms and conditions according to their true intent and meaning for an amount to be determined in accordance with the conditions of contract identified in the Contract Data.

THE OFFERED TOTAL OF THE PRICES INCLUSIVE OF VAT IS:

(in words) _____

(in figures) R _____

The Tenderer confirms that he has read the Contract referred to in C1.2 Contract Data.

This Offer may be accepted by the Employer by signing the Acceptance part of this Form of Offer and Acceptance and returning one copy of this document to the Tenderer before the end of the period of validity stated in the Tender Data, whereupon the Tenderer becomes the party named as the Contractor in the Conditions of Contract identified in the Contract Data.

Signature(s) _____

Name(s) _____

Capacity _____

For the Tenderer:

(Insert name and address of organisation)

Name & Signature of Witness _____

Date _____

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)

C1.1 FORM OF OFFER AND ACCEPTANCE

B: ACCEPTANCE

By signing this part of the Form of Offer and Acceptance, the Employer identified below accepts the Tenderer's Offer. In consideration thereof, the Employer shall pay the Contractor the amount due in accordance with the Conditions of Contract identified in the Contract Data. Acceptance of the Tenderer's Offer shall form an agreement between the Employer and the Tenderer upon the terms and conditions contained in this Agreement and in the Contract that is the subject of this Agreement.

The terms of the contract are contained in:

- C.1 Agreement, and Contract Data, (which include this Agreement)
- C.2 Pricing Data, including the Bill of Quantities
- C.3 Scope of Work
- C.4 Site Information and drawings and documents or parts thereof, which may be incorporated by reference into the above listed Parts.
- C.5 Annexures.
 - o Annexure A Occupational Health and Safety Specification
 - o Annexure B ISMS Tender Drawings & Specifications
 - o Annexure C Form of Design Indemnity
 - o Annexure D Cession of Rights

Deviations from and amendments to the documents listed in the Tender Data and any addenda thereto listed in the Tender Schedules as well as any changes to the terms of the Offer agreed by the Tenderer and the Employer during this process of offer and acceptance, are contained in the Schedule of Deviations attached to and forming part of this Agreement. No amendments to or deviations from said documents are valid unless contained in this Schedule, which must be duly signed by the authorised representatives of both parties.

The Tenderer shall within two weeks after receiving a completed copy of this Agreement, including the Schedule of Deviations (if any), contact the Employer's agent (whose details are given in the Contract Data) to arrange the delivery of any other bonds, guarantees, proof of insurance and any other documentation to be provided in terms of the Conditions of Contract identified in the Contract Data. Failure to fulfil any of these obligations in accordance with those terms shall constitute a repudiation of this Agreement.

Notwithstanding anything contained herein, this Agreement comes into effect on the date when the Tenderer receives one fully completed original copy of this document, including the Schedule of Deviations (if any). Unless the Tenderer (now Service Provider) within five days of the date of such receipt notifies the Employer in writing of any reason why he cannot accept the contents of this Agreement, this Agreement shall constitute a binding contract between the parties.

Signature: *(of person authorised to sign the acceptance)*

Name: *(of signatory in capitals)*

Capacity: *(of Signatory)*

Name of Employer: *(organisation)*

Address:

Telephone number: _____ **Fax number:** _____

AS WITNESS

Signature: _____ **Name:** *(in capitals)* _____

Date: _____

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)

C1.1 FORM OF OFFER AND ACCEPTANCE (CONTINUED)

C: SCHEDULE OF DEVIATIONS

The extent of deviations from the tender documents issued by the Employer prior to the tender closing date is limited to those permitted in terms of the Tender Data and the Conditions of Tender.

A Tenderer's covering letter will not necessarily be included in the final contract document. Should any matter in such letter, which constitutes a deviation as aforesaid become the subject of agreements reached during the process of offer and acceptance, the outcome of such agreement shall be recorded here.

Any other matters arising from the process of offer and acceptance either as a confirmation, clarification or change to the tender documents and which it is agreed by the Parties becomes an obligation of the contract shall also be recorded here.

Any change or addition to the tender documents arising from the above agreements and recorded here shall also be incorporated into the final draft of the Contract.

1. **Subject:** _____
Details: _____

2. **Subject:** _____
Details: _____

3. **Subject:** _____
Details: _____

4. **Subject:** _____
Details: _____

5. **Subject:** _____
Details: _____

6. **Subject:** _____
Details: _____

By the duly authorised representatives signing this Schedule of Deviations, the Employer and the Tenderer agree to and accept the foregoing Schedule of Deviations as the only deviations from and amendments to the documents listed in the Tender Data and addenda thereto as listed in the Tender Schedules, as well as any confirmation, clarification or change to the terms of the offer agreed by the Tenderer and the Employer this process of offer and acceptance.

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)

C1.1 FORM OF OFFER AND ACCEPTANCE (CONTINUED)

C: SCHEDULE OF DEVIATIONS

It is expressly agreed that no other matter whether in writing, oral communication or implied during the period between the issue of the tender documents and the receipt by the Tenderer of a completed signed copy of this Agreement shall have any meaning or effect in the contract between the parties arising from this Agreement.

FOR THE TENDERER:

Signature: _____

Name: _____

Capacity: _____

Tenderer: *(Name and address of organisation)*

Witness:

Signature: _____

Name: _____

Date: _____

FOR THE EMPLOYER

Signature: _____

Name: _____

Capacity: _____

Witness:

Signature: _____

Name: _____

Date: _____

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)

C1.2 CONTRACT DATA

C1.2.1 GENERAL CONDITIONS OF CONTRACT

1. FORM OF CONTRACT

The JBCC (Joint Building Contracts Committee) Principal Building Agreement – Edition 6.2 – May 2018”, as amended in the SPECIAL CONDITIONS OF CONTRACT, shall be applicable to this contract.

2. PRELIMINARIES

The JBCC (Joint Building Contracts Committee) General Preliminaries - May 2018, as amended in the SPECIAL CONDITIONS OF CONTRACT, shall be applicable to this contract.

3. TRADE PREAMBLES

The “General Preambles for Trades (2017 Edition)”, as recommended by The Association of South African Quantity Surveyors shall apply to this contract and is obtainable from The Association of South African Quantity Surveyors or Building Industries Federation South Africa (BIFSA).

4. PRINCIPAL BUILDING AGREEMENT CONTRACT DATA

The details are stated in the schedule named “Principal Building Agreement Contract Data”.

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)

C1.2.2 SPECIAL CONDITIONS OF CONTRACT

1. GENERAL

These special Conditions of Contract generally contain clauses that are either deemed to be additions, elaborations or variations to the General Conditions of Contract. Accordingly, these Special Conditions of Contract must be read in conjunction with the General Conditions of Contract and it shall be deemed that the amended meanings and intentions of the clauses shall apply, if applicable. In addition, it shall be deemed that any reference to Contractor shall mean Principal Building Contractor, as defined in the JBCC Principal Building Agreement.

2. SCOPE OF THE CONTRACT

The scope of the contract for each Tender option/s, if applicable, is described in the Specifications, Drawings, Bills of Quantities, Contract Conditions and the Contract Variables, as applicable.

3. CONFIDENTIALITY

It shall be deemed that the details of the contract documents shall be treated as private and confidential and their general content shall not be disclosed or discussed with third parties without the prior approval of the Principal Agent in writing.

The contractor undertakes to maintain in confidence any and all information regarding this project and shall obtain appropriate similar undertakings from all subcontractors and suppliers. Such information shall not be used in any way except in connection with the execution of the works. No information regarding this project shall be published or disclosed without the prior written consent of the Employer.

4. PROGRAMME

The Contractual Commencement and Completion dates and any other relevant dates for this contract are stated in the "JBCC PRINCIPAL BUILDING AGREEMENT: CONTRACT DATA".

Time, cost and quality are to be considered the essence of this Contract. Accordingly, it shall be deemed that the contract programme prepared and issued in Microsoft Project Programming Software, detailing each activity and duration is submitted by the Contractor, in accordance with the tender requirements, and as amended in conjunction with the Principal Agent and/ or other Agents, shall be the basis of monitoring progress on the project. The programme is to include construction activities, long lead procurement schedules, information required schedules, tenant information schedules and sub-contractor appointment schedules.

The Process to be adopted in finalising the programme shall be as follows:

- The Construction Project Manager and/ or Principal Agent shall evaluate the programme to ensure the completeness of the work programmed, accuracy of the durations, relevance and completeness of the logic, dates on which information are requested, times allowed for long lead items and subcontractor appointment dates.
- Any shortcomings and/ or further requirements shall be clearly indicated in a programme assessment report and issued to the contractor for correction and additions.
- The contractor shall effect amendments to the programme based on the above and the final contract programme shall be signed-off by the Project Team and shall be deemed to be the baseline/ target contract programme. This programme, and the progress therein, (and relevant authorised revisions), will form the basis of adjudication of all clauses relating to time as specified in the contract document. The submission of the programme and the dates therein shall not excuse or relieve the principal building contractor or its parties from completing the project within the timeframe specified in the contract documents.

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)

C1.2.2 SPECIAL CONDITIONS OF CONTRACT (CONTINUED)

4. PROGRAMME (CONTINUED)

- The contractor shall update the contract/project programme at any time when the works been developed do not, or may not correspond to that originally programmed, or as formally instructed by the Project Manager and/ or Principal Agent. It shall be deemed that the principal building contractor has, when updating or developing the programme, consulted with the relevant project team members as well as the relevant nominated and selected sub-contractors regarding procurement period, specifications and sequencing required.

The process to be adopted for **PROGRESS REVIEW** shall be as follows:

- The Project Manager and/ or Principal Agent, and the Contractor shall conduct a progress review on a pre-determined weekly interval. The progress for each activity of the works shall be evaluated, agreed upon and recorded in a report.
- The progress review shall incorporate procurement of long lead items, information release, fit-out information and sub-contractor appointments.

The following information shall be recorded for each activity:

- Actual start dates of the planned activities (if started),
- Actual finish dates of the planned activity (if completed),
- Estimated remaining durations of the planned activities that are still in progress,
- Suspend and resume dates if a planned activity is suspended, and
- Log text of delays incurred to planned activities.

The result after the progress update must be closely evaluated and the relevance and accuracy of the results must be checked.

NOTE:

- The Contractor is not permitted to make any changes to the Contract Programme without agreement by the Project Manager and/ or Principal Agent.
- Extension of time claims due to inclement weather, late information, or any other reason shall far as practical, be evaluated the moment it is submitted and the effect on the contractual end date determined.
- A decision shall as far as practical be made immediately on the number of days to be granted to the contractor, if any.
- Claims that have no effect on the critical path shall be so recorded.
- A summary of the extension of time claims submitted, for both inclement weather and contractual claims must be included in the joint progress report.

5. DAMAGE TO THE WORK

Care shall be taken not to cause any damage to any part of the existing or new work or any adjoining property. The contractor will be held responsible for damage caused to the works by his negligence and shall be liable for all costs incurred in making good any such damage to the satisfaction of the Principal Agent.

6. COMMUNICATION, MEDIA RELEASES, ETC.

The contractor shall not in any way communicate with the press, or any representative of the written or electronic media, on a question affecting this contract unless prior approval in writing is received from the Employer and/ or the Principal Agent.

All rights of publication of articles in the media, together with any advertising relating to, or in any way concerned with this project shall vest in the Employer.

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)

C1.2.2 SPECIAL CONDITIONS OF CONTRACT (CONTINUED)

The contractor shall not, without the written consent of the Principal Agent, cause any statement or advertisement to be printed, screened or aired by the media.

7. COPYRIGHT

No part of this document and any document forming part of the contract documents may be copied, photographed or repeated in any manner or by any process without the written consent of the **author**. Copyright is reserved on all designs, specifications, patents and patentable designs, systems and processes contained in documents pertaining to this contract. The person, firm, body, supplier, contractor, sub-contractor and any other contracting party is to be responsible jointly and severally, in their personal and corporate capacities for any contravention of this requirement.

8. ESCALATION

This contract shall be a **Fixed Price** and is **not subject to any CPAP (Contract Price Adjustment Provisions)**.

FOR CONSIDERATION

This contract shall **be subject to Contract Price Adjustment Formulae such as the Haylett Formulae or similar, after a period of 12 months since tender closing has elapsed (subject to agreement between the successful tenderer and client)**, which shall be dependent on the tender offer accepted. In this regard, it is deemed that for the fixed price option, the contract amount includes for any potential increases (except any variation in the rate of value added tax) in the cost of labour, materials, transport, etc.

The option applicable to this contract is as indicated below:

Option 1 – Subject to Escalation Price Contract

TBC

Option 2 – Fixed Price Contract

Key: ☒ - Tender Option Applicable
☒ - Not Required for this Tender

Fixed for
12 months

9. WORKMANSHIP AND QUALITY CONTROL

The Contractor shall execute the work in accordance with and as described in the document referenced as "Construction Works: Specifications, as prepared by the Department: Public Works Republic of South Africa – PW 371, EDITION 2.0 July 2013". The document is freely available for download from the website www.publicworks.gov.za.

The contractor shall, at his own expense, institute a quality control system and provide other technical staff, together with all transport, instruments and equipment to ensure adequate supervision and positive control of the works at all times.

The cost of supervision and process control, including testing carried out by the contractor shall be deemed to be included in the amount quoted for the works.

The contractor's attention is drawn to the normal standards (as prescribed by SANS 10400 and amplified in 'General Preambles to Trades [2017] and trade specific modification thereto) regarding the minimum frequency of testing required for materials. The contractor shall, at his own discretion increase this frequency where necessary to ensure adequate control.

On completion and submission of every part of the work to the **Principal Agent** for examination, the contractor shall furnish the **Principal Agent** with the results of the relevant tests, measurements and levels to indicate compliance with the specifications.

Notwithstanding the approval of these above-mentioned tests by the **Principal Agent**, the contractor shall remain solely responsible for the work as defined in this contract document, up to the end of the defect's liability period.

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)

10. REPORTING OF ACCIDENTS/ INCIDENTS

In addition, to any statutory obligations the contractor shall, as soon as practical, report to the Principal Agent every occurrence on the works or the site causing damage to the property or injury or death to any individuals. If requested, the contractor shall submit a report in writing to the Principal Agent within 12 hours of such request, setting out the full details of the occurrence. The Principal Agent shall have the right to make any enquiries either on the site or elsewhere as to the cause and results of any such occurrence and the contractor shall render all reasonable assistance and make available the necessary facilities, equipment, personnel, etc., for carrying out such enquiries.

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)

1.2.2 SPECIAL CONDITIONS OF CONTRACT (CONTINUED)

11. IDENTIFICATION OF PERSONNEL

All personnel that are utilised on the project by the contractor and its sub-contractors, are at all times whilst on site, be clothed with clothing that clearly identifies each staff member together with an identification document which includes, but not limited to the following:

- A photograph of the personnel concerned;
- The identification numbers of the personnel concerned; and,
- The name of company concerned

In addition, to that stated above, the contractor shall adhere to the premises security rules and regulations. No personnel will be permitted to work on the project until this condition is adhered to.

All personnel must have valid RSA identification documentations and have successfully passed all client required security checks.

Refer to Stage 04 – Security Verification for full details.

12. INTERVENTION AT MANUFACTURE AND/ OR SUPPLIER AND/ OR SUB-CONTRACT LEVEL

The employer and its agents reserve the right to discuss and liaise on any issue pertaining to this contract with the contractor's service providers i.e. Manufacturers and/ or suppliers and/ or sub-contractors concerned (Nominated and Selected and Domestic). This right shall not create privity of the contract between the employer and/ or its agents and the said manufacturer and/ or supplier and/ or sub-contractors, (Nominated and Selected and Domestic).

13. ALTERATIONS IN THE QUANTITY AND VALUE OF WORK

The employer and/ or its Agents shall be permitted to either increase or decrease the quantity and value of work contracted for. In this regard, the contractor including its service providers shall not be entitled to claim for any additional expense incurred, or for any change in the rates for work done and/ or any materials and services supplied. It shall be deemed that all costs associated with this item is included in the Contract Sum.

14. CHANGES IN THE SCOPE OF WORK

The contractor acknowledges that whilst drawings have been prepared for this project, the scope of work and value of the contract may be substantially altered and that no claims for loss and expense shall be due by the employer for implementing any changes that may become necessary. It shall be deemed that the contract amount includes for all costs that may arise due to compliance with this clause.

15. MARKET RELATED WAGE RATES

The wage rates payable for labour in any category is deemed to be not less than the lessee of:

- Statutory wage rates in any labour category in the project locality; and
- The SAFCEC, NBCEI or similar recommended minimum rates applicable at any time during the duration of the contract.

The Contractor shall demonstrate compliance with this requirement on a monthly basis.

16. TREASURES, RELICS, ETC.

Any relics, treasure, articles of value or of potential historical or archaeological interest found on the site must be brought to the attention of the **PRINCIPAL AGENT**. All work at the specific area of the discovery shall stop for a reasonable time period until such time that the **PRINCIPAL AGENT** instructs the contractor to continue with the work.

Any relics, treasure, articles of value or of potential historical or archaeological interest found on the site shall remain the property of the Employer and shall be handed over to the **PRINCIPAL AGENT** who shall be the sole arbitrator of what is an article of value.

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)

C1.2.2 SPECIAL CONDITIONS OF CONTRACT (CONTINUED)

17. PRICED BILLS OF QUANTITIES

The Contractor shall submit the Priced Bills of Quantities at the date of the tender closing.

18. LUMP SUM PRICE BREAKDOWN

Where items in the Tender document are measured as lump sums, the contractor shall, upon request submit a detailed Priced Bills of Quantities for each lump sum item **WITHIN TEN (10) DAYS OF NOTICE OF AWARD OF CONTRACT**, which shall be prepared in accordance with the latest edition of the standard system of Measuring Building Work including any subsequent amendments thereto, which will thereafter form part of the contract and shall be used for the purposes of preparing valuation certificates, determining the value of variation orders, preparation of final account, etc.

19. PRICES AND NET MEASUREMENTS

Prices throughout these bills of quantities shall be deemed to include for all obligations arising out of the contract and unless otherwise specified, be held to include for making, conveying and delivering, unloading, storing, unpacking, hoisting, setting, fitting and fixing in position, cutting and waste, patterns, models and templates, plant, temporary works and return of packing's.

Prices for all items contained in these bills of quantities and any additional authorised variations, shall be deemed to exclude all amounts due in terms of the Value-Added Taxation Legislation. A provision for the addition of VAT shall be made on the summary page of the contract document and final statement of accounts, as applicable.

20. AMENDMENTS TO SCOPE OF WORK PRIOR TO TENDER AWARD

The Contractor is advised that certain portions of the scope of work may be adjusted/ omitted subject to the Client's approval of the adjustments/ omissions and can only be affected prior to the issuance of the Letter of Intent to Award. Any cost associated with the imminent scope change must be included in the overall price, as claims for additional costs/ loss and expense will not be entertained.

21. WARRANTIES

The contractor undertakes to perform the work in accordance with the terms and the conditions of the contract, in a workmanlike manner, which shall include but not be limited to, complying with the manufacturers/ suppliers' specifications, if applicable, in respect of goods, methods, or materials used in the performance of the work.

The contractor further warrants that they shall use only new merchantable materials, fit for their intended purpose, as well as supervision, labour and equipment which are fit for the purpose for which they are intended.

22. OVERLOADING

The contractor shall take all necessary steps to ensure that no damage occurs due to overloading of any portion of the works or temporary works e.g. scaffolding, etc. The contractor shall submit details of his proposed loading, storage, plant erection, etc., to the Principal Agent for approval prior to proceeding with such loading, storing or erecting and shall comply with and pay for the Principal Agent's requirements in connection with the provision of temporary support work, etc. Any damage caused to the works by overloading shall be made good by the contractor at his sole expense.

23. BLACK ECONOMIC EMPOWERMENT

The contractor shall comply with the Employers Black Economic Empowerment Policies.

24. ADVERTISING RIGHTS

The Employer may elect to contract with advertising agencies for the erection of advertising hoardings, banners, wraps or the like for the duration of the contract. The contractor shall not prevent such an arrangement and will assist in the facilitation of same. The position and type of advertising structure to be agreed with the Principal Agent so as not to hinder the contractor in meeting his obligations under this agreement.

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)

C1.2.2 SPECIAL CONDITIONS OF CONTRACT (CONTINUED)

25. MEDIA RELEASES

All rights of publication of articles in the media, together with any advertising relating thereto or in any way connected with this project, shall vest with the Employer. The contractor together with his subcontractors shall not, without the prior written consent of the Employer, cause any statement or advertisement connected with this project to be printed, screened or aired by the media.

26. STANDARD OF WORKMANSHIP AND MATERIALS

In the absence of detailed specifications for any item or items, National Building Regulations, the latest applicable SANS 2001 Standards for Construction Works shall apply, or where such does not exist, then the latest applicable British Standard Specification (BS) shall apply.

Suppliers of materials and the like, whose quality systems apply with one or more of the SABS/SANS ISO 9000 Series should be used whenever possible in the absence of a particular SABS/SANS Specification Standard Mark.

27. EXISTING PREMISES OCCUPIED

Where circumstances arise that the works programmed to be executed interferes with the general routine of the occupants, the contractor is to advise the Principal Agent forty-eight (48) hours before the commencement of said works.

Notwithstanding anything to the contrary in the agreement, the contractor acknowledges that access to the works and sections after the date of practical completion is subject to the prior consent of the Principal Agent, and in turn subject to the consent of the occupants or management of that part of works.

28. PROTECTION

All surfaces, particularly those that remain unfinished such as stone work, existing original tiles/floor finishes, timber work etc., should be kept safe from damage and protected where necessary. Where protection is used this should be made out of soft board or plywood boards and must not be directly fixed to the area that is being protected. Corners of window frames, sandstone projections etc. should be protected from damage, particularly in high traffic areas.

All ironmongery, fittings or materials temporarily removed to aid the construction process or for safe keeping from potential damage should only be done so with the express permission of the architect and heritage consultant. These should be individually labelled and packed for safe keeping and future re-installation.

29. SITE WORKS

The site should be kept secure at all times.

Areas used for the storage of building materials, establishing of a site office, parking etc. are to be confirmed with the architect and heritage consultants.

The extents of the area being used for building works should be clearly defined and no works, storage or disposal of materials should occur beyond these.

Caution should be taken when delivering materials and accessing the site to ensure that no damage is done to the existing building, retain walls etc.

30. FALSE DECLARATION

All information provided by the contractor is accepted in good faith as being true and accurate. Any false declaration or intentional omission of relevant facts shall be reported to the Employer, which on receipt of such report may elect to exercise its (the employer's) rights in terms of common law and/ or the contract, as applicable.

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)

C1.2.2 SPECIAL CONDITIONS OF CONTRACT (CONTINUED)

31. ACCESS FOR PERSONNEL

No unauthorised persons are allowed on site unless authorised by the DTIC in writing. No persons are allowed access to any portion of the existing buildings, if applicable, other than the agreed entrance and exit routes, unless authorised by the Principal Agent in writing.

The contractor shall provide access permits for staff and vehicles, uniforms, PPE, identification cards for all personnel accessing the area of the works, including subcontractors.

32. SUPERVISION BY EMPLOYER'S AGENTS

Supervision by the Principal Agent and other agents is intended as a means of checking the interpretation of work done and providing clarification and further information where required during the progress of the work. Supervision shall not in any way relieve the contractor of his responsibility for ensuring that the work is carried out satisfactorily in all aspects, in good time and in accordance with the contract.

Although the Principal Agent and other agents will make spot checks from time to time on dimensions and levels as the work proceeds, checking of the setting out, dimensions, levels and positioning of all items is the contractor's responsibility and should any errors occur during the course of or be found after completion of the works, the cost for remedying same will be for the contractor's account.

33. PARTNERING

The Employer, its agents and the contractor shall act as stated in the contract and in the spirit of mutual trust and co-operation. In this regard, it is a specific requirement that all the contractor's personnel provide reasonable assistance that may be required by the Employer and/ or its agents in order for them to assist in bringing the works to completion with due skill, diligence, regularity and expedition. In turn, the Employer and its agents shall also provide assistance to the contractor to execute the works with due skill, diligence, regularity and expedition.

In turn, the Employer and its agents shall also provide assistance to the contractor to execute the works with due skill, diligence, regularity and expedition.

34. TESTING AND COMMISSIONING

The Contractor shall provide the tests in accordance that described in the document referenced as "Construction Works: Specifications, as prepared by the Department: Public Works Republic of South Africa – PW 371, EDITION 2.0 July 2013".

The contractor and / or sub-contractors shall commission and test the entire installation at his own expense, including provision of electrical power supplies, water supplies, fuel and all test equipment. Such testing is to be done in the presence of the Principal Agent, who shall have been notified of the dates and approximate duration of the tests, sufficiently in advance so as to allow attendance at such tests.

35. CONTRACTORS RESPONSIBILITY

The Employer, the Principal Agent and the other professional consultants shall not be responsible for any act or omission on the part of the contractor which may result in any patent or latent defects, in materials or workmanship, breach or neglect of any local regulations. The contractor shall at all times be responsible for any such neglect, deviation or wrong act, whether the same is discovered before or after the final certificate, or any other certificate, has been approved.

36. METHOD STATEMENT

The contractor shall produce, when required to do so by the Principal Agent, a method statement outlining the methods of construction and labour and plant resources that he proposes to use in the execution of the works. Any approval given or observation made by the Principal Agent shall not relieve the contractor of his sole responsibility to adopt the methods of construction and to provide the labour and plant resources necessary for the due and proper timeous execution of the works. The method statement developed shall be project specific.

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)

C1.2.2 SPECIAL CONDITIONS OF CONTRACT (CONTINUED)

37. QUALITY CONTROL AND QUALITY ASSURANCE

The contractor shall be required to provide suitably qualified and experienced staff capable of executing the work to the required standard and quality.

Definitions

The following definitions are applicable:

Quality Policy: The overall intentions and direction of an organisation as regards quality.

Quality System: The organisational structures, responsibilities, procedures, processes and resources for implementing quality policy.

Quality Control: The operational techniques and activities that are used to fulfil requirements of quality.

Quality Assurance: All those planned and systematic actions necessary to provide adequate confidence that a product or service will satisfy given requirements for quality.

38. QUALITY CONTROL AND QUALITY ASSURANCE (CONTINUED)

General:

The contractor shall submit his quality policy and comprehensive quality system proposals prior to appointment and within one week of being requested by the Principal Agent to do so. The quality system shall be drawn up to meet the requirements set out herein and incorporating all additional requirements and controls the contractor considers necessary for effective quality control and assurance of products and service. The contractor shall provide dedicated and experience staff capable for implementing the proposed quality system.

The Principal Agent shall comment on the quality system within two weeks of receipt of same from the contractor, outlining additions or amendments considered necessary for acceptance of the quality systems. The contractor shall meet with the Principal Agent and amend the contents of the quality systems according to the Principal Agent's comments.

Amendments to the system shall be made within one week of the Principal Agent's comments. Upon final acceptance of the quality system, it shall form a quality manual which shall, inter alia, contain the following:

- Quality policy.
- Organisational goals and structures.
- Internal audit plan incorporating resources, documentation, procedures and processes, etc.
- Record keeping.
- Reports: format and content.
- Follow up actions and audit finding.
- Testing: including outside testing by CSIR, SANS, PCI and others.
- Measurement control.
- Non-conformance: identification, review, corrective action, prevention of recurrence, etc.

The acceptance of the quality system by the Principal Agent does not supersede or negate any other quality control conditions stipulated elsewhere in the contract documents and in the instance of contradiction of requirements being identified, specific requirements shall override general requirements. Acceptance of the system by the Principal Agent shall not in any way supersede, negate or alter the intent, content or interpretation of the specification or conditions of contract specified elsewhere in the contract documents. Acceptance of the system by the Principal Agent does not in any way relieve the contractor of his responsibility to satisfy the conditions of contract and to achieve and maintain the specified standards. The quality system is an audit procedure and does not necessarily describe the contractor's total responsibility in terms of quality control.

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)

C1.2.2 SPECIAL CONDITIONS OF CONTRACT (CONTINUED)

38. QUALITY CONTROL AND QUALITY ASSURANCE (CONTINUED)

The Principal Agent may from time to time call for the quality control assurance data sheets for random checking of:

- The manner in which the system is being administrated
- The technical acceptability of the contents of the sheets, and
- The effectiveness of the system in controlling the attainment of the required end product.

If the system is found to be inadequate or ineffective the Principal Agent will have the right to declare the system or parts thereof as being areas of "non-performance". In the event of the Principal Agent instructing the contractor by an architect's instruction of an area of "non-performance" the following options may be implemented by the principal agent at no additional costs to the employer and without any claim for delays.

The structure for approval may be altered necessitating the signature of quality control and assurance data sheets by designated agents before work of a particular nature and/or in a particular area can proceed through the various check stages of the system.

The structure of the system may be altered by extending the detail of checking required by the system and/or the frequency at which check sheets have to be produced.

The geographical boundaries of a typical checking operation may be altered thereby requiring the contractors to perform more comprehensive checks on smaller portions of the work.

The contractor shall react immediately to an instruction by the Principal Agent regarding any alteration to the procedure of the system. On receipt of an instruction on any non-performance from the Principal Agent the contractor shall not proceed with any of the affected work until acceptance of the revised procedure has been obtained from the Principal Agent.

Once the Principal Agent is satisfied that the revised quality control and assurance procedures are effective, the contractor will be informed by means of an official Principal Agent's instruction of the extent to which the system may revert to the principle of management by exception. It is envisaged that the system should generally operate on such a basis and providing the results are satisfactory, the contractor is not expected to attain approval by countersignature of every quality control data sheet.

In instances where up-front inspection is an industry norm (e.g., inspection of reinforcing by the structural engineer) or where the specification demands such inspection, the contractor must take this into account when compiling the quality control system.

It is envisaged that "samples and mock-ups" shall be extensively used to define the accepted standards of workmanship and materials to be used. The contractor shall also prepare and maintain a register of all samples indicating numbers, date, bill of quantities and specification reference, approval and relevant documents. The Principal Agent will submit a quality report indicating areas of concern with regard to the quality of the project. The contractor is to remedy the works within a two-week period or supply the Principal Agent with a programme indicating the duration of remedial work for specific items. Such programme will be subject to the reasonable approval of the Principal Agent.

39. OMISSION FOR WORK FOR WHICH PROVISIONAL SUMS HAVE BEEN ALLOWED

The selected / nominated subcontract amounts allowed in these bills of quantities include work to be executed in accordance with employer's requirements. The contractor accepts that, such work may, at the Principal Agent's discretion, be omitted from this contract and executed under separate contract/s. In such case, the contractor shall allow access to the handed over areas of the works to allow such separate contractors to proceed with such work prior to handover and/or expiry of the defect's liability period.

The contractor hereby accepts that he shall not be entitled to any profit mark-up on the omitted work and that no claim for loss of profit shall be entertained.

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)

C1.2.2 SPECIAL CONDITIONS OF CONTRACT (CONTINUED)

40. SPECIAL TASKS

The Employer shall have the right to employ other contractors to execute any special tasks whether contained in this contract or not, concurrently with the works being executed under this contract.

The contractor shall not be entitled to any profit and / or builder's discount on the value of any work executed by other contractors but shall nevertheless allow these other contractors and the Employer's employees to have access to the works, allocate reasonable space for the storage of their materials, tools and equipment.

Without in any way detracting from the generality of or limiting the above, the contractor is advised that the special tasks will be carried out by the Employer and other contractors and the value of such work shall not be included in this contract.

41. INTERPRETATION OF THE DRAWINGS, SPECIFICATIONS AND BILLS OF QUANTITIES

The contractor shall be held solely responsible for and shall, at his own expense, rectify any errors arising out of the incorrect interpretation of the Drawings, Specifications, Bills of Quantities or Instructions.

Should any part of the Drawings, Specifications or Bills of Quantities not be clearly intelligible to the contractor, or the material or articles to be used in the execution of the works be considered insufficiently described or the manner in which the work is to be carried out not clear, the contractor must obtain from the Principal Agent the necessary information to clarify such Drawings, Specifications, Bills of Quantities or Instructions, which request shall be in writing.

All drawings, whatever their origin, are to be issued to the site or to any other person or persons only through the Principal Agent's office and shall bear the Principal Agent's office stamp and signature and an up to date register of all drawings issued to the contractor shall be kept on the works. Any other drawings used on the site will be used at the contractor's risk and should any work be incorrect due to the use of unauthorised drawings the cost of rectifying such work shall be for the contractor's account.

All drawings used on the works shall be properly mounted on suitable sheet material or otherwise protected and kept in good condition. Any drawings becoming bleached or otherwise obscured so that they cannot be properly read shall be returned to the Principal Agent for replacement, as any errors due to misreading of damaged or obscured drawings shall be made good by the contractor at his own expense.

Precedence of documentation

1. Contract Data
2. Specifications
3. Drawings
4. Bill Of Quantities

42. AVAILABILITY OF MANAGEMENT PERSONNEL

It shall be deemed that the contractor has allowed in the contract amount for the Construction Project Manager / Site Agent, Senior Foreman, Quantity Surveyor, and Construction Health and Safety Officer for the management of direct contracts, throughout the direction of the contract. Such persons are to be available to attend meetings to resolve any contractual and other related issues within 24 (twenty-four) hours on receipt of notice, either written or verbal, from the Principal Agent.

43. LOCAL LABOUR

It is deemed that the contractor shall, as far as possible, maximise the use of labour from the area in which the project is located.

44. REMOVAL AND MAKING GOOD TEMPORARY WORKS ETC. ON COMPLETION

The contractor shall remove (except where specifically stated otherwise) all temporary works, roads, hoardings, services and the like used for this contract and shall make good to the entire satisfaction of the Principal Agent any damage resulting therefrom.

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)

C1.2.2 SPECIAL CONDITIONS OF CONTRACT (CONTINUED)

45. EQUALLY APPROVED MATERIAL

Where reference is made to a particular trade name or product, the Tenderer is to note that the term equally approved applies in all instances. Where the Tenderer chooses to investigate and price a product that they consider to be equally approved to that stated, the Tenderer is required to provide evidence consisting of Drawings, specifications and product catalogues with their Tender. Such information needs to satisfy the adjudicators that the alternative proposed is in fact equally approved. The Client is not obliged to accept any alternative proposed.

46. PRECONTRACT ENGAGEMENT

Contractors shall be engaged prior to issuance of site possession to facilitate all necessary precontract work which shall include the construction work permit application, procurement of specialist sub-contractors, finalisation of contract and any design coordination between the contractor and the professional team. Contractors will be required to make the necessary allowances for such work during this period as no claims for additional preliminaries will be entertained.

47. SPECIFIC PRELIMINARIES

Contractors are to refer to the specific preliminaries contained within the priced bills of quantities.

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)

C1.2.3 PRINCIPAL BUILDING AGREEMENT CONTRACT DATA

The Clause References and Principal Contract Data provided in the table below must be read in conjunction with the Standard JBCC Principal Contract Data Form for Information provided by the Employer.

A PROJECT INFORMATION

A 1.0 Works [1.1]

Project Name	APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)
Contract Reference Number	RFP002-2025/26
Works Description	Integration of the campus systems. The project scope is further defined in part C3 of the bid document.

A 2.0 Site [1.1]

Erf / Stand Number	86
Township / Suburb	Trevenna
Site Address	77 Meintjies Street, Sunnyside, Pretoria, Gauteng
Local Authority	City of Tshwane Metropolitan Municipality

A 3.0 Employer [1.1]

Name	Rainprop RF (Pty) Ltd		
Legal Entity of Above	Rainprop RF (Pty) Ltd		
Country	Republic of South Africa		
Contact Person	Khaya Ncwana		
Telephone Number	012 440 6900		
Email	khaya@rainprop.co.za		
Postal Address	77 Meintjies Street, Block B Ground Floor, The Dtic Campus, Sunnyside, Pretoria	Code	0002
Physical Address	77 Meintjies Street, Block B Ground Floor, The Dtic Campus, Sunnyside, Pretoria	Code	0002

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)

C1.2.3 PRINCIPAL BUILDING AGREEMENT CONTRACT DATA (CONTINUED)

A 4.0

A 13.0 Electronic Engineer (ISMS) [1.1; 6.2]

Name	SAJ Engineering		
Legal Entity of Above	Private Company		
Country	Republic of South Africa		
Contact Person	Steyn de Lange		
Telephone Number	073 660 6012		
Email	steyndelanges@outlook.com		
Postal Address	99 Featherview, Falls Road, Mogale City	Code	1759
Physical Address	99 Featherview, Falls Road, Mogale City	Code	1759

C1.2.3 PRINCIPAL BUILDING AGREEMENT CONTRACT DATA (CONTINUED)

B CONTRACT INFORMATION

B 1.0 Definitions [1.1]

Bills of Quantities: System/ Method of measurement	N/A
---	-----

B 2.0 Law, Regulations and Notices [2.0]

Law applicable to the works, state country [2.1]	Republic of South Africa
---	--------------------------

B 3.0 Offer and Acceptance [3.0]

Currency applicable to this agreement [3.2]	South African Rand (R)
--	------------------------

B 4.0 Documents [5.0]

The original signed agreement is to be held by the principal agent [5.2], if not, indicate by whom	The Client: Rainprop RF (Pty) Ltd
Number of copies of contract information issued to the contractor at no cost [5.6]	Two (2)
Documents comprising the agreement	Page numbers
The JBCC® Principal Building Agreement, Edition 6.2 May 2018	1 to 30
The JBCC® Principal Building Agreement - Contract Data for Organs of State and other Public Sector Bodies, Edition 6.2 May 2018	1 to 14

APPOINTMENT OF A CONTRACTOR FOR THE REFURBISHMENT FOR THE INTEGRATED SECURITY SOLUTION AND IMPLEMENTATION FOR the dtic CAMPUS, TRAVENNA, SUNNYSIDE PRETORIA FROM THE TENDER (RFP002-2025/26)

The JBCC® General Preliminaries for use with the JBCC® Principal Building Agreement, Edition 6.2 May 2018	1 to 7
The Priced Bill of Quantities	BOQ 116 to BOQ 126

Contract drawings – description	Number	Revision	Date
Refer to Annexure B for Tender Drawings & Specifications	-	-	-

B 5.0 Employer's Agents [6.0]

Authority is delegated to the following agents to issue contract instructions and perform duties for specific aspects of the works [6.2]
Electronic Engineer (ISMS)

Principal agent's and agent's interest or involvement in the works other than a professional interest [6.3]
None

C1.2.3 PRINCIPAL BUILDING AGREEMENT CONTRACT DATA (CONTINUED)

B 6.0 Insurances [10.0]

Insurances by employer			Amount including tax	Deductible amount including tax
Contract works insurance:				
	New works [10.1.1] (contract sum or amount)		N/A	-
Or	Works with practical completion in sections [10.2] (contract sum or amount)		N/A	-
Or	Works with alterations and additions [10.3] (reinstatement value of existing structures with or including new works)		N/A	-
	Direct contractors [10.1.1; 10.2] where applicable, to be included in the contract works insurance		N/A	-
	Free issue [10.1.1; 10.2] where applicable included in the contract works insurance		N/A	-
	Escalation, professional fees and reinstatement costs if not included above		N/A	-
Total of the above contract works insurance amount			N/A	-
Supplementary insurance [10.1.2; 10.2]			N/A	-
Public liability insurance [10.1.3; 10.2]			N/A	-
Removal of lateral support insurance [10.1.4; 10.2]			N/A	-
Other insurances [10.1.5]			N/A	-
Yes/ no?		If yes, description 1	N/A	-
Yes/ no?		If yes, description 2	N/A	-

C1.2.3 PRINCIPAL BUILDING AGREEMENT CONTRACT DATA (CONTINUED)**B CONTRACT INFORMATION (CONTINUED)****B 6.0 Insurances [10.0] (Continued)**

And/ or

Insurances by contractor			Amount including tax	Deductible amount including tax
Contract works insurance:				
	New works [10.1.1] (contract sum or amount)		N/A	N/A
or	Works with practical completion in sections [10.2] (contract sum or amount)		N/A	N/A
or	Works with alterations and additions [10.3] (reinstatement value of existing structures with or including new works)		To the minimum value of the Contract Sum + 20% per claim	With a deductible not exceeding 5% of each and every claim
	Direct contractors [10.1.1; 10.2] where applicable, to be included in the contract works insurance		N/A	-
	Free issue [10.1.1; 10.2] where applicable included in the contract works insurance		N/A	-
	Escalation, professional fees and reinstatement costs if not included above		N/A	-
Total of the above contract works insurance amount			To the minimum value of the Contract Sum + 20% per claim	minimum value of R60 000.00
Supplementary insurance [10.1.2] (SASRIA)			R 30 Million	R 50 000.00
Public liability insurance [10.1.3]			R 30 Million	R 50 000.00
Removal of lateral support insurance [10.1.4]			N/A	N/A
Other insurances [10.1.5]				
Yes/ no?	No	If yes, description 1	N/A	N/A

C1.2.3 PRINCIPAL BUILDING AGREEMENT CONTRACT DATA (CONTINUED)**B 7.0 Obligations of the employer [12.1]**

Existing premises will be in use and occupied [12.1.2]		Yes/ no?	Yes
If yes, description	Operational campus with employees. Building under construction will be empty.		
Restriction of working hours [12.1.2]		Yes/ no?	Yes
If yes, description	The completion of the project is urgent, and work shall be executed during normal working hours i.e. 7h00 until 17h00 daily including weekends. Work required to be executed outside of these hours must be arranged with the Principal Agent , in advance.		
Natural feature and known services are to be preserved by the contractor [12.1.3]		Yes/ no?	No
If yes, description	To be indicated at the compulsory briefing and at site handover		
Restrictions to the site or areas that the contractor may not occupy [12.1.4]		Yes/ no?	Yes
If yes, description	Work areas and restricted areas shall be defined at the compulsory briefing and at site handover Further restrictions to site access All employees of the contractor and his sub contractors to be RSA citizens All employees, sub contractors to follow the below procedure: 1.0 The principal agent will collect and submit the following documents from the contractor to the dtic VFU: Applicant Consent form - signed and dated Declaration of Secrecy – signed and dated Copy of valid RSA Identification document. (all workers to be RSA citizens) 2.0 an appointment for the contractors to come for electronic fingerprints to the VFU. At least two weeks before the commencement of the works. Mondays and Tuesdays between 09h00 and 12h45. (20 people per day) 3.0: The VFU will submit the fingerprints to the service provider and the balance of the days of the week would be reasonable sufficient time for the service provider to provide feedback on the fingerprints and the VFU to evaluate the outcome.		
Supply of free issue [12.1.10]		Yes/ no?	No
If yes, description	Not Applicable		

B 8.0 Nominated subcontractors [14.0]

Specialisation 1	Not Applicable
Specialisation 2	Not Applicable
Specialisation 3	Not Applicable
Specialisation 4	Not Applicable

B 9.0 Direct Contractors [16.0]

Extent of work [12.1.11]	
Extent of work [12.1.11]	

B 10.0 Description of sections [20.1]

(The block numbers referenced has no bearing to the actual building names.)

Section 1	Block 1
Section 2	Block 2
Section 3	Block 3
Section 4	Block 4
Section 5	Block 5
Section 6	Block 6
Section 7	Block 7

B 11.0 Possession of site [12.1.5], practical completion [19.0; 20.0] and penalties [24.0]

Practical completion for the works as a whole	Intended date of possession of the site [12.1.5]	Period for inspection by the principal agent [19.3]	Date for practical completion [12.2.7; 24.1]	Penalty [24.1]
	Date	Working days	Date	Penalty amount per calendar day
	N/A	N/A	N/A	N/A

Or where sections are applicable

The overall contract period is 24 months. The sections below display the duration per block. There will be 30 days/month hard stop between each block to allow for the block to be emptied and work to start.

Practical completion of a section of the works	Intended date of possession of a section [12.1.5]	Period for inspection by the principal agent [19.3]	Date for practical completion [12.2.7; 24.1]	Penalty [24.1]
	Date	Working days	Date	Penalty amount per calendar day
Section 1		7 DAYS	75 days	0.031% of the contract sum
Section 2		7 DAYS	75 days	0.031% of the contract sum
Section 3		7 DAYS	75 days	0.031% of the contract sum
Section 4		7 DAYS	75 days	0.031% of the contract sum
Section 5		7 DAYS	75 days	0.031% of the contract sum
Section 6		7 DAYS	75 days	0.031% of the contract sum
Section 7		7 DAYS	100 days	0.031% of the contract sum

C1.2.3 PRINCIPAL BUILDING AGREEMENT CONTRACT DATA (CONTINUED)

Criteria to achieve practical completion not covered in the definition of practical completion
On achievement of practical completion, the contractor is to hand over certificates and manuals, etc. related to the works as listed below: • Electrical Certificate of Compliance. • SANS 10222-2 Compliance • All documentation to comply with statutory and legislative requirements. • Draft handover pack ○ As-built drawings ○ Commissioning data ○ Operating and maintenance manuals ○ Training register

B 12.0 Payment [25.0]

Date of month for issue of regular payment certificates [25.2]	30th	
Cost fluctuations [25.3.4; 26.9.5]	Yes/ no?	No
If yes, method to calculate		

B 13.0 Dispute Resolution [30.0]

Adjudication [30.6.1; 30.10] Name of nominating body	To be agreed between parties
Applicable rule for adjudication [30.6.2]	Adjudication in accordance with the CIDB adjudication process
Arbitration [30.7.4; 30.10] Name of nominating body	As appointment by the Chairman of the Association of Arbitrators South Africa
Applicable rule for arbitration [30.7.5]	as determined by the appointed Arbitrator

C1.2.3 PRINCIPAL BUILDING AGREEMENT CONTRACT DATA (CONTINUED)**B CONTRACT INFORMATION (CONTINUED)****B 14.0 JBCC General Preliminaries – selections**

Provisional bills of quantities [P2.2]		Yes/ no?	Yes
Availability of construction information [P2.3]		Yes/ no?	Yes
Previous work – dimension accuracy – details of previous contract(s) [P3.1]		The Contractor to verify all dimensions on site and report any discrepancies.	
Previous work – defects – details of previous contract(s) [P3.2]		The Contractor is to inspect and document all defects in a form of report prior to commencement of the works.	
Inspection of adjoining properties – details [P3.3]		The Contractor is to inspect all adjoining structures and document all defects in a form of report prior to commencement of the works.	
Handover of site in stages – specific requirements [P4.1]		Refer to B 11.0 (Contract Data)	
Enclosure of the works – specific requirements [P4.2]		Hoarding off to working areas. Dust and noise disturbance to all buildings are not in construction or being worked on.	
Geotechnical and other investigations – specific requirements [P4.3]		Not Applicable	
Existing premises occupied – details [P4.5]		Working Areas will not be occupied. Adjacent buildings will be occupied and operational.	
Services – known – specific requirements [P4.6]		None	
Water [P8.1]	By contractor	Yes/ no?	Yes
	By employer	Yes/ no?	No
	By employer – metered	Yes/ no?	No
Electricity [P8.2]	By contractor	Yes/ no?	Yes
	By employer	Yes/ no?	No
	By employer – metered	Yes/ no?	No
Ablution and welfare [P8.3]	By contractor	Yes/ no?	Yes
	By employer	Yes/ no?	No
Communication facilities – specific requirements [P8.4]		Email, Telephone, etc.	
Protection of the works – specific requirements [P11.1]		The Contractor is to protect the works undertaken by others from damage during the execution of the contract. The cost of rectification as a result of any damages, should they occur, shall be for the contractor's account.	
Protection/ isolation of existing works and works occupied in sections – specific requirements [P11.2]		If Applicable the Contractor maybe required to provide hoarding to areas of works, in accordance with the Principal Agent's instructions.	
Disturbance – specific requirements [P11.5]		As prescribed in the General Preliminaries	
Environmental disturbance – specific requirements [P11.6]		Refer to Annexure A Occupational Health and Safety Specifications	

C1.2.3 PRINCIPAL BUILDING AGREEMENT CONTRACT DATA (CONTINUED)**B CONTRACT INFORMATION (CONTINUED)****B 15.0 Changes made to JBCC Documentation**

Clause 1.0 - Definitions and interpretation
Pricing of bills of quantities
The contractor is to allow opposite each item for all costs in connection therewith. All prices to include, unless otherwise stated, for all materials, fabrication, conveyance and delivery, unloading, storing, unpacking, hoisting, labour, setting, fitting and fixing in position, cutting and waste (except where to be measured in accordance with the standard system of measurement), patterns, models and templates, plant, temporary works, returning of packaging, duties, taxes (other than Value Added Tax), imposts, establishment charges, overheads, profit and all other obligations arising out of this agreement. Value Added Tax (VAT) is to be separately stated on the summary page of these bills of quantities
Items left unpriced will be deemed to be covered in prices against other items throughout these bills of quantities and no claim for any extras arising out of the contractor's omission to price any item will be entertained
Prices for all construction equipment, temporary works, services and other items shall include for the supply, maintenance, operating cost and subsequent removal and making good as necessary
Abbreviated descriptions
The items in these bills of quantities utilise abbreviated descriptions. It is the intention that the abbreviated descriptions be fully described when read with the applicable measuring system and the relevant preambles and/or specifications. However, should the full intent and meaning of any description not be clear, the contractor shall, before submission of his tender, call for a written directive from the principal agent, failing which it shall be assumed that the contractor has allowed in his pricing for materials and workmanship in terms of international best practice
Legal status of contractor
If the contractor constitutes a joint venture, consortium or other unincorporated grouping of two or more persons then:
1. These persons are deemed to be jointly and severally liable to the employer for the performance of this agreement
2. These persons shall notify the employer of their leader who has assigned authority to bind the contractor and each of these persons
3. The contractor shall not alter its composition or legal status without the prior written consent of the employer
Clause 5.0 - Documents
Value Added Tax
Provision is made in the summary page of these bills of quantities for the inclusion of Value Added Tax (VAT)
Electronic issue of drawings All drawings for this project will be issued electronically and the contractor shall be deemed to have received such drawings on the date that such drawings have been dispatched electronically [5.6]
Clause 6.0 - Employer's agents
Delegated authority:
The authority of the principal agent to issue contract instructions [17.1] and perform duties for specific aspects of the works is delegated to agents as follows [6.2]. This does not preclude the principal agent from issuing such contract instructions:
1. Architect
1.1 Duties [6.2] : The architect is responsible for the architectural design, functional design and quality inspection of the works
1.2 Contract instructions [6.2; 17.1] :
1.2.1 Rectification of discrepancies, errors in description or quantity or omission of items in the agreement other than in the JBCC Principal Building Agreement
1.2.2 Alteration to design, standards or quantity of the works provided that such contract instructions shall not substantially change the scope of the works
1.2.3 The site [13.0]
1.2.4 Compliance with the law, regulations and by laws [2.1]
1.2.5 Provision and testing of samples of materials and goods and/or of finishes and assemblies of elements of the works

C1.2.3 PRINCIPAL BUILDING AGREEMENT CONTRACT DATA (CONTINUED)**B CONTRACT INFORMATION (CONTINUED)****B 15.0 Changes made to JBCC Documentation (Continued)**

1.2.6	Opening up of work for inspection, removal or re-execution [23.2.4; 26.4.2]
1.2.7	Removal or re-execution of work
1.2.8	Removal or substitution of any materials and goods
1.2.9	Protection of the works
1.2.10	Making good physical loss and repairing damage to the works [23.2.2]
1.2.11	Rectification of defects [21.2]
1.2.12	A list for practical completion specifying outstanding or defective work to be rectified to achieve practical completion, a list for completion and a list for final completion specifying outstanding or defective work to be rectified to achieve final completion
1.2.13	Expenditure of budgetary allowances, prime cost amounts and provisional sums
1.2.14	Appointment of a subcontractor [14.0; 15.0]
1.2.15	Work by direct contractors [16.0]
1.2.16	On suspension or termination, protection of the works, removal of construction equipment and surplus materials and goods [29.0]
1.2	Contract instructions [6.2; 17.1] :
1.2.1	Rectification of discrepancies, errors in description or quantity or omission of items in the agreement other than in the JBCC Principal Building Agreement
2.	Quantity surveyor
2.1	Duties [6.2] : The quantity surveyor is responsible for all measurements, valuations, financial assessments and all other quantity surveying and cost control functions of the works
2.2	Contract instructions [6.2; 17.1] :
2.2.1	No contract instructions shall be delegated to the quantity surveyor
2.2.2	Rectification of discrepancies, errors in descriptions or omissions in contract documents other than this agreement.
2.2.3	Alteration to design, standards or quantity of the works provided that such contract instructions shall not substantially change the scope of the works.
2.2.4	Expenditure of budgetary allowances, prime cost amounts and provisional sums.
3.	Civil and structural engineer
3.1	Duties [6.2] : The civil and structural engineer is responsible for all aspects of civil and structural engineering design and quality inspection of the works
3.2	Contract instructions [6.2; 17.1] :
3.2.1	Rectification of discrepancies, errors in description or quantity or omission of items in the agreement other than in the JBCC Principal Building Agreement
3.2.2	Alteration to design, standards or quantity of the works provided that such contract instructions shall not substantially change the scope of the works
3.2.3	The site [13.0]
3.2.4	Compliance with the law, regulations and by laws [2.1]
3.2.5	Provision and testing of samples of materials and goods and/or of finishes and assemblies of elements of the works
3.2.6	Opening up of work for inspection, removal or re-execution [23.2.4; 26.4.2]
3.2.7	Removal or re-execution of work
3.2.8	Removal or substitution of any materials and goods
3.2.9	Protection of the works
3.2.10	Making good physical loss and repairing damage to the works [23.2.2]
3.2.11	Rectification of defects [21.2]
3.2.12	A list for practical completion specifying outstanding or defective work to be rectified to achieve practical completion, a list for completion and a list for final completion specifying outstanding or defective work to be rectified to achieve final completion
3.2.13	Expenditure of budgetary allowances, prime cost amounts and provisional sums

C1.2.3 PRINCIPAL BUILDING AGREEMENT CONTRACT DATA (CONTINUED)**B CONTRACT INFORMATION (CONTINUED)****B 15.0 Changes made to JBCC Documentation (Continued)**

4. Mechanical engineer
4.1 Duties [6.2] : The mechanical engineer is responsible for all aspects of mechanical engineering design and quality inspection of the works and, where appointed by the employer for quantity surveying services in respect of the mechanical installations, for all measurements, valuations, financial assessments and all other quantity surveying and cost control functions
4.2 Contract instructions [6.2; 17.1] :
4.2.1 Rectification of discrepancies, errors in description or quantity or omission of items in the agreement other than in the JBCC Principal Building Agreement
4.2.2 Alteration to design, standards or quantity of the works provided that such contract instructions shall not substantially change the scope of the works
4.2.3 Compliance with the law, regulations and by laws [2.1]
4.2.4 Provision and testing of samples of materials and goods and/or of finishes and assemblies of elements of the works
4.2.5 Opening up of work for inspection, removal or re-execution [23.2.4; 26.4.2]
4.2.6 Removal or re-execution of work
4.2.7 Removal or substitution of any materials and goods
4.2.8 Protection of the works
4.2.9 Making good physical loss and repairing damage to the works [23.2.2]
4.2.10 Rectification of defects [21.2]
4.2.11 A list for practical completion specifying outstanding or defective work to be rectified to achieve practical completion, a list for completion and a list for final completion specifying outstanding or defective work to be rectified to achieve final completion
4.2.12 Expenditure of budgetary allowances, prime cost amounts and provisional sums
4.2.13 Appointment of a subcontractor [14.0; 15.0]
4.2.14 Termination of a nominated n/s subcontract agreement [27.2.8]
4.2.15 Work by (a) direct contractor(s) [16.0]
4.2.15 Access by other or previous contractors to remedy defective work.
4.2.17 Removal from the site of any person employed on the works
4.2.18 Removal from the site of any person not engaged on or connected with the works
4.2.19 On termination, protection of the works, removal of construction equipment and surplus materials and goods [29.0]
5. Electrical engineer
5.1 Duties [6.2] : The electrical engineer is responsible for all aspects of electrical engineering design and quality inspection of the works and, where appointed by the employer for quantity surveying services in respect of the electrical installations, for all measurements, valuations, financial assessments and all other quantity surveying and cost control functions
5.2 Contract instructions [6.2; 17.1] :
5.2.1 Rectification of discrepancies, errors in description or quantity or omission of items in the agreement other than in the JBCC Principal Building Agreement
5.2.2 Alteration to design, standards or quantity of the works provided that such contract instructions shall not substantially change the scope of the works
5.2.3 Compliance with the law, regulations and by laws [2.1]
5.2.4 Provision and testing of samples of materials and goods and/or of finishes and assemblies of elements of the works
5.2.5 Opening up of work for inspection, removal or re-execution [23.2.4; 26.4.2]
5.2.6 Removal or re-execution of work
5.2.7 Removal or substitution of any materials and goods
5.2.8 Protection of the works
5.2.9 Making good physical loss and repairing damage to the works [23.2.2]
5.2.10 Rectification of defects [21.2]
5.2.11 A list for practical completion specifying outstanding or defective work to be rectified to achieve practical completion, a list for completion and a list for final completion specifying outstanding or defective work to be rectified to achieve final completion
5.2.12 Expenditure of budgetary allowances, prime cost amounts and provisional sums

C1.2.3 PRINCIPAL BUILDING AGREEMENT CONTRACT DATA (CONTINUED)**B CONTRACT INFORMATION (CONTINUED)****B 15.0 Changes made to JBCC Documentation (Continued)**

5.2.13 Appointment of a subcontractor [14.0; 15.0]
5.2.14 Termination of a nominated n/s subcontract agreement [27.2.8]
5.2.15 Work by (a) direct contractor(s) [16.0]
5.2.15 Access by other or previous contractors to remedy defective work.
5.2.17 Removal from the site of any person employed on the works
5.2.18 Removal from the site of any person not engaged on or connected with the works
5.2.19 On termination, protection of the works, removal of construction equipment and surplus materials and goods [29.0]
6. Fire consultant
6.1 Duties [6.2] : The fire consultant is responsible for all aspects of rational fire design and quality inspection of the works
6.2 Contract instructions [6.2; 17.1] :
6.2.1 Rectification of discrepancies, errors in description or quantity or omission of items in the agreement other than in the JBCC Principal Building Agreement
6.2.2 Alteration to design, standards or quantity of the works provided that such contract instructions shall not substantially change the scope of the works
6.2.3 Compliance with the law, regulations and by laws [2.1]
6.2.4 Provision and testing of samples of materials and goods and/or of finishes and assemblies of elements of the works
6.2.5 Opening up of work for inspection, removal or re-execution [23.2.4; 26.4.2]
6.2.6 Removal or re-execution of work
6.2.7 Removal or substitution of any materials and goods
6.2.8 Protection of the works
6.2.9 Making good physical loss and repairing damage to the works [23.2.2]
6.2.10 Rectification of defects [21.2]
6.2.11 A list for practical completion specifying outstanding or defective work to be rectified to achieve practical completion, a list for completion and a list for final completion specifying outstanding or defective work to be rectified to achieve final completion
6.2.12 Expenditure of budgetary allowances, prime cost amounts and provisional sums
6.2.13 Appointment of a subcontractor [14.0; 15.0]
6.2.14 Termination of a nominated n/s subcontract agreement [27.2.8]
6.2.15 Work by (a) direct contractor(s) [16.0]
6.2.15 Access by other or previous contractors to remedy defective work.
6.2.17 Removal from the site of any person employed on the works
6.2.18 Removal from the site of any person not engaged on or connected with the works
4.2.19 On termination, protection of the works, removal of construction equipment and surplus materials and goods [29.0]
7. Wet services engineer
Note that the contract instructions hereinafter are selected from those listed in clause 17.1 of the JBCC PBA
7.1 Duties [6.2] : The wet services engineer is responsible for all aspects of wet services engineering design and quality inspection of the works
7.2 Contract instructions [6.2; 17.1] :
7.2.1 Rectification of discrepancies, errors in description or quantity or omission of items in the agreement other than in the JBCC Principal Building Agreement
7.2.2 Alteration to design, standards or quantity of the works provided that such contract instructions shall not substantially change the scope of the works
7.2.3 Compliance with the law, regulations and by laws [2.1]
7.2.4 Provision and testing of samples of materials and goods and/or of finishes and assemblies of elements of the works
7.2.5 Opening up of work for inspection, removal or re-execution [23.2.4; 26.4.2]
7.2.6 Removal or re-execution of work
7.2.7 Removal or substitution of any materials and goods
7.2.8 Protection of the works
7.2.9 Making good physical loss and repairing damage to the works [23.2.2]

C1.2.3 PRINCIPAL BUILDING AGREEMENT CONTRACT DATA (CONTINUED)**B CONTRACT INFORMATION (CONTINUED)****B 15.0 Changes made to JBCC Documentation (Continued)**

7.2.10 Rectification of defects [21.2]
7.2.11 A list for practical completion specifying outstanding or defective work to be rectified to achieve practical completion, a list for completion and a list for final completion specifying outstanding or defective work to be rectified to achieve final completion
7.2.12 Expenditure of budgetary allowances, prime cost amounts and provisional sums
8. Electronic engineer
8.1 Duties [6.2] : The electronic engineer is responsible for all aspects of electronic engineering design and quality inspection of the works and, where appointed by the employer for quantity surveying services in respect of the electronic installations, for all measurements, valuations, financial assessments and all other quantity surveying and cost control functions
8.2 Contract instructions [6.2; 17.1] :
8.2.1 Rectification of discrepancies, errors in description or quantity or omission of items in the agreement other than in the JBCC Principal Building Agreement
8.2.2 Alteration to design, standards or quantity of the works provided that such contract instructions shall not substantially change the scope of the works
8.2.3 Compliance with the law, regulations and by laws [2.1]
8.2.4 Provision and testing of samples of materials and goods and/or of finishes and assemblies of elements of the works
8.2.5 Opening up of work for inspection, removal or re-execution [23.2.4; 26.4.2]
8.2.6 Removal or re-execution of work
8.2.7 Removal or substitution of any materials and goods
8.2.8 Protection of the works
8.2.9 Making good physical loss and repairing damage to the works [23.2.2]
8.2.10 Rectification of defects [21.2]
8.2.11 A list for practical completion specifying outstanding or defective work to be rectified to achieve practical completion, a list for completion and a list for final completion specifying outstanding or defective work to be rectified to achieve final completion
8.2.12 Expenditure of budgetary allowances, prime cost amounts and provisional sums
Where it is expected of the contractor to waive his lien in terms of clause 11.10, the waiver of lien may be extended to subcontracts as follows:
The contractor shall ensure that a waiver of lien is included in all subcontracts and that the works executed on the site are kept free of all liens and other encumbrances at all times [11.10]
Clause 11.0 is deemed to be amended by the addition of the following new sub-clauses: Sub-clause 11.11 - The guarantee provided by the contractor's Guarantor shall have an expiry date (if stated) no less than 3 months after the practical completion date and shall be extended accordingly should the practical completion date be extended. The cost for same shall be included on the contractor's tender price as no claims for additional cost shall be entertained.
Clause 12.0 - Obligations of the parties
Office accommodation: The contractor shall provide, maintain and remove on practical completion air conditioned office accommodation with suitable tables and chairs for meetings to be held on the site. Such offices shall be kept clean and fit for use at all times [12.2.18] The contractor's site camp shall be equipped with Wi-Fi internet connection which shall be utilised by the contractor's staff, the client and members of professional team.

C1.2.3 PRINCIPAL BUILDING AGREEMENT CONTRACT DATA (CONTINUED)**B CONTRACT INFORMATION (CONTINUED)****B 15.0 Changes made to JBCC Documentation (Continued)**

Notice board The contractor shall erect in a position approved by the principal agent, maintain and remove on practical completion a notice board recommended by the South African Institute of Architects and as approved by the principal agent listing the names and logos of the employer, the contractor and the professional consultants. No subcontractor or supplier notice boards may be erected unless permission is granted by the principal agent for such notice boards to be erected [12.2.18]
Statutory and other notices
The contractor shall submit and/or comply with all statutory and other notices that may be required by any local or other authority in order not to cause any delay to the commencement of the works by the contractor. The contractor shall pay all deposits or fees in this regard
It is, however, specifically recorded that the employer shall be responsible for the timeous approval of building plans by any local or other authorities and the payment of any fees or charges related thereto
Sub-clause 12.2.6 is deemed to be amended by the addition of the following new sub-clauses: The programme for the works must be prepared and issued in Microsoft Project Programming Software. The contractor shall include a float of 15 working days within the contract period for project delays such as, but not limited to adverse weather conditions, etc., in the programme. Such provisions shall initially be included at the end of the contract period or proportionally allocate at the end of each section for contracts with sectional completion and shall be monitored by the contractor and agreed with the Principal Agent as and when such delays takes place and shall be recorded in the programme based on actual stoppages when incurred. Revision of the date for Practical Completion shall only be considered once the 15 working days has been fully utilised. Notwithstanding the above, any and all float that may arise through early completion of any activities shall belong to the project and not any one party.
Sub-clause 12.2.10 is deemed to be amended by the addition of the following new sub-clauses: The contractor shall be required to maintain, in addition to the approved programme, a comprehensive fortnightly bar-chart programme expanded to reflect anticipated daily activities for the ensuing fourteen (14) days.
Clause 16.0 – Direct contractors Attendance on direct contractors In respect of direct contractors the contractor shall:
1. Designate an area for the direct contractor to establish a temporary office and workshop and storage of equipment and materials
2. Allow the use of personnel welfare facilities, where provided
3. Provide water, lighting and single phase electric power to a position within 50m of the place where the direct contract work is to be carried out, other than fuel or power for commissioning of any installation
4. Permit the direct contractor to use erected scaffolding, hoisting facilities, etc provided by the contractor, in common with others having the like right, while it remains erected on the site [16.1]
Clause 17.0 – Contract instructions
Contract instructions: Instructions issued on site are to be recorded in a site instruction book which is to be supplied and maintained on site by the contractor.
Clause 17.0 is deemed to be amended by the addition of the following new sub-clauses: 17.1.21 Acceleration.
Clause 19.0 – Practical completion
Clause 19.0 is deemed to be amended by the addition of the following new sub-clauses: Sub-clause 19.2.3 – The contractor shall within five (5) calendar days of receipt of the list for practical completion issue a programme indicating dates for completion for all listed items.
Sub-clause 19.2.4 – In the event that such inspection does not result in the work being accepted as practically complete, then the costs of such inspection and subsequent inspections shall be for the account of the contractor, at a rate of Ten Thousand Rand (R10 000.00) per man hour or part thereof, calculated by multiplying the total of the number of Employer's agents and Employer's staff present at each abortive practical completion inspection meeting, i.e. Where practical completion is not achieved, by the time taken for such an inspection until practical completion is achieved. In this regard, the Employer reserves the right to recover such costs in addition to any other remedies it may have in accordance with Clause 27.

C1.2.3 PRINCIPAL BUILDING AGREEMENT CONTRACT DATA (CONTINUED)

B CONTRACT INFORMATION (CONTINUED)

B 15.0 Changes made to JBCC Documentation (Continued)

Clause 21.0 – Defects liability period and final completion
Clause 21.0 is deemed to be amended by the addition of the following new sub-clauses: Sub-clause 21.13 – In the event that the certificate of Final Completion is not issued due to the contractor's work not being sufficiently complete then the costs of such inspection and subsequent inspections shall be for the account of the contractor, at a rate of Ten Thousand Rand (R10 000.00) per man hour or part thereof, calculated by multiplying the total of the number of Employer's agents and Employer's staff present at each abortive final completion inspection meeting, i.e. Where final completion is not achieved in terms of 21.6, by the time taken for such an inspection until final completion is achieved. In this regard, the Employer reserves the right to recover such costs in accordance with Clause 27.
Sub-clause 21.14 - Notwithstanding [21.2], where the contractor fails to rectify/attend to outstanding works or defects on the list for completion, list for final completion or latent defects that appear before the issue of certificate of final completion and where the contractor remains in default, the Employer may engage others to carry out said outstanding works or defects and recover expense and/or loss incurred [27].
Clause 23.0 - Revision of the date for practical completion
Sub-clause 23.1 is deemed to be amended by the addition of the following new sub-clauses: Sub-clause 23.1.7 - Delayed possession of site [12.1.5].
Sub-clause 23.2 is deemed to be amended by the omission of the following new sub-clauses: Sub-clause 23.2.1 Delayed possession of the site [12.1.5].
Clause 23.0 is deemed to be amended by the addition of the following new sub-clauses: "The contractor is instructed to allow for ten (10) working days during the contract period for the delay due to circumstances as listed in Clauses 23.1.1 to 23.1.6, in the programming of the works. Extensions to the contract completion date will only be considered arising for the above delays, after the actual delays recorded and accepted by the principal agent exceed (10) ten days so allowed."
Clause 23.0 is deemed to be amended by the addition of the following new sub-clauses: "23.9 Acceleration 23.9.1 Irrespective of whether or not the principal agent rules that the contractor is entitled to an extension of time or a revision of the date for practical or sectional completion, the principal agent shall nevertheless at any time, be entitled to instruct the contractor, to accelerate the progress of the remaining works, to ensure that the works are completed by the original date for practical or sectional completion or revised date as the case may be.
23.9.2 Upon receipt of such instruction, the contractor shall take necessary steps to ensure that the works are completed timeously, including the provision by him of additional resources, plant, manpower, etc. and working overtime or additional overtime beyond that contemplated at the time of tender (at all times adhering to the regulations and requirements of all authorities) and by all other adequate and proper means methods. The contractor shall prove that such steps are being taken if called upon to do so.
23.9.3 Should the principal agent instruct the contractor to accelerate works, the contractor's additional entitlement shall be calculated by adding the entitlement to which he would otherwise have become due should the construction period have been extended, a further 30% to the value thereof. For the purpose of the calculation of 30% acceleration entitlement relating to an extension of construction period granted in terms of Clause 23.1 shall be calculated as if the extension was granted in terms of 23.2.
Substitution of materials and goods The removal or substitution of any materials and goods which do not conform to the specification or the contract drawings shall not constitute grounds for the extension of the construction period nor for the adjustment of the contract value [17.1.8; 23.1 & 2]
Clause 23.0 is deemed to be amended by the addition of the following new sub-clauses: Sub-clause 23.10 - Notwithstanding, sub-clause(s) 23.1 to 23.8 a revision to the practical completion date will only be considered for work on the critical path of the contractual programme or the revised contractual programme, as applicable. Any revised programme, in order to be considered as a contractual programme, must be approved by the Principal Agent in writing, prior to it becoming effective.

C1.2.3 PRINCIPAL BUILDING AGREEMENT CONTRACT DATA (CONTINUED)**B CONTRACT INFORMATION (CONTINUED)****B 15.0 Changes made to JBCC Documentation (Continued)**

Clause 25.0 – Payment
Prices submitted Where prices are submitted by the contractor or subcontractor during the progress of the works in respect of contract instructions or in regard to a claim under the terms of this agreement and notwithstanding the fact that such prices may be used in an interim payment certificate, there is to be no presumption of acceptance. Should the principal agent wish to accept any such prices prior to the issue of the certificate of final completion, it shall be in writing
Sub-clause 25.1 has been amended to include the following: The contractor shall submit the following information on a monthly basis to the Principal Agent and Quantity Surveyor in order to assist with the processing of the payment certificate and the preparation of the empowerment report: A detailed breakdown of the work done. (The work breakdown must be referenced strictly in accordance with the Tender Document or the detailed Priced Bills of Quantities, as applicable); A detailed breakdown of all variation order costs claimed (With specific reference to work done by the Principal Building Contractor) in the certificate concerned, together with copies of the relevant contract instructions; A detailed breakdown of the work done by each sub-contractor. (The work breakdown must be referenced strictly in accordance with the Tender Document or the detailed Priced Bills of Quantities, as applicable.); A detailed breakdown of all variation order costs claimed in the certificate concerned for sub-contract work, together with copies of the relevant contract instructions; A written declaration authenticated by the contracts manager confirming, that the payment claims for work done by sub-contractors has been audited and amended by the contractor's quantity surveyor, prior to it being forwarded to the Principal Agent and Quantity Surveyor for evaluation; If applicable, a combined empowerment report which shall include reports on contractor and sub-contractor compliance, in accordance with the format required by the empowerment manager. In this regard, the combined, contractor and sub-contractor empowerment report must contain an affidavit certifying that all information contained the report as being true and correct and must be authenticated by the contractor and a commissioner of oaths. The combined reports must also state that the contractor has checked and verified that all information submitted by sub-contractors is true and correct; Tax invoice: the contractor shall attach a tax invoice as prescribed in the value added tax legislation to each payment certificate when presenting the certificate to the employer for payment. Such tax invoices shall correctly reflect the prescribed information and the amounts shall match precisely the amounts included in the payment certificate. Should the contractor fail to comply with these requirements, the date of presentation of the certificate shall be deemed to be delayed at the contractor's default until such time as the requirements are met.
Sub-clause 25.4 has been amended to include the following: Where the Employer agrees to pay for materials on site, the contractor shall be required to provide the Principal Agent with the necessary forms for cession of ownership for such materials (Annexure D), with the necessary delivery notes and invoices (where applicable).
Clause 25.10 is deemed to be deleted and replaced with the following: "The employer shall pay the contractor the amount certified in the issued payment certificate within thirty (30) calendar days of the date for issue of the payment certificate [CD] including interest".
Clause 26.0 - Adjustment of the contract value and final account
Sub-clause 26.1 is deemed to be amended by the addition of the following new sub-clauses: Contract Instructions - Instructions given by the Employer's agents in relation to the contract works, shall, irrespective of the format or wording of such instructions, not indicate that the work involved represents an extra or variation and shall not be deemed to be acceptance of any prices or quotations contained in any correspondence. It is recorded that only the quantity surveyor where appointed by the employer for quantity surveying services is empowered, to rule whether any instructions issued constitutes an extra or not and, to resolve cost aspects of any matter pertaining to this contract.
Fluctuations in costs All fluctuations in costs, with the exception of fluctuations in the rate of Value Added Tax, shall be for the account of the contractor [26.9.5]
The employer reserves the right to omit such work without compensation to the contractor for loss of profit or any other loss which the contractor may suffer as a result of such omission.

C1.2.3 PRINCIPAL BUILDING AGREEMENT CONTRACT DATA (CONTINUED)**B CONTRACT INFORMATION (CONTINUED)****B 15.0 Changes made to JBCC Documentation (Continued)**

Cost of claims All costs incurred by the contractor in the preparation of claims shall be borne by the contractor. This provision shall not preclude an adjudicator or an arbitrator appointed in terms of this agreement [30.6 & 7] from making a determination on costs
Claims from subcontractors The contractor shall review, assess and adjudicate any claims received by him from any subcontractor and thereafter submit same to the principal agent with a recommendation in order to assist the principal agent in adjudicating the claim [26.6]
Clause 30.0 - Dispute resolution.
Agreement
The required information of the parties and the amount of the contract sum shall be inserted in the agreement for signature of the agreement by the parties.
Contract data
Tenderer's selections
Before submission of his tender the contractor is to complete the tenderer's selections in the contract data
Clause 2.1 - Checking of documents
Sub-clause 2.1 refers – the following is to be added after the words “written directive”: The items in these Bills of Quantities are to be read and priced in conjunction with, and the descriptions regarded as amplified by the General Preambles for Trades 2017 as recommended and published by the Association of South African Quantity Surveyors, 2017 edition, and no claim arising from brevity of description of items fully described in the said General Preambles for Trades 2017 and Supplementary documentation will be entertained. Notwithstanding the issue of the tender drawings, it will remain the responsibility of the Tenderer to study all available drawings at the offices of the Principal Agent during normal working hours in order to acquaint himself with all the cost implications of the design, programming, phasing, etc.
Clause 2.2 - Provisional bills of quantities
The quantities in provisional bills of quantities are an indication of the works to be executed and are subject to remeasurement
Multiple procurement These bills of quantities are in multiple procurement format i.e. the "wet trades" - earthworks, concrete, formwork and reinforcement, precast concrete, masonry, waterproofing and sub-surface drainage - are provisionally measured and the subsequent trades are budgetary allowances and/or provisional sums.
Clause 4.2 - Enclosure of the works
Describe any specific hoarding requirements, other than already described in clause 4.2 or in the contract data
Clause 5.1 - Management of the works
Clause 5 has been amended to include the following new sub-clause: Sub-clause 5.4 - Daily records - The contractor shall keep daily records of people and equipment employed as well as a site diary in respect of work performed on the site. At the end of each week the contractor shall provide the Principal Agent with a written record, in schedule form, reflecting the number and description of tradesmen and labourers employed by him and all sub-contractors on the works each day. At the end of each week the contractor shall provide the Principal Agent with a written record, in schedule form, reflecting the number, type and capacity of all plant, excluding hand tools, currently used on the works.
Clause 6.2 - Workmanship samples
Sub-clause 6.2 has been amended to include the following: The contractor shall provide a mock-up of all finished surfaces prior to commencement of the relevant work. The contractor shall only be permitted to commence with the relevant scope of work, on approval of the mock-up by the Principal Agent or its designated representative.

C1.2.3 PRINCIPAL BUILDING AGREEMENT CONTRACT DATA (CONTINUED)**B CONTRACT INFORMATION (CONTINUED)****B 15.0 Changes made to JBCC Documentation (Continued)**

Clause 6.3 - Shop drawings
Sub-clause 6.3 refers – the following is to be added after the words 'and/or approval': Shop drawings shall be submitted to the principal agents for approval at least ten (10) working days weeks prior to the date on which such approval is required in order to comply with the programme. All submissions shall be prepared in accordance with the contract drawings and specifications and/or any Principal Agents instructions and any deviation shall be specifically highlighted in writing, with a detailed explanation of the reason for such deviation, together with any cost and/or time implications. Delays in approval of shop drawings due to non-compliance with drawings, specifications and/or Principal Agent's instruction shall not constitute grounds for any claims for delay, extension of time and the like. The contractor shall be responsible for ensuring that all dimensions affecting shop drawings conform to the dimensions of built work. Should the contractor, sub-contractor, supplier or manufacturer be of the opinion that corrections to shop drawings made by the Principal Agent, constitute a change to the scope of work, then he shall immediately advise the Principal Agent in writing of this, together with the cost and/or programme implications thereof, in order to obtain the Principal Agent's directive.
Sub-clause 6.3.1 has been amended as follows: Replace the words "two (2) copies" with "four (4) copies" under bullet point number 6.
Clause 10.1 - General attendance General attendance is defined as being the duties of the contractor in terms of clause 12.2 of the JBCC n/s subcontract agreement
Clause 10.2 - Special attendance
Sub-clause 10.2 has been amended to include the following: The Tenderer shall examine all drawings and information pertaining to the works as a whole and shall provide all necessary special attendance resources required for the due and proper execution and completion of all sub-contract works.
Clause 11.5 – Disturbance
Disturbance All demolition work including removal thereof to dispatch areas as well as other works that will cause excessive noise, dust and odour shall only take place after hours between 18h00 and 06h00. Any delays, stoppages and the like arising from or in order to comply with the above will not constitute grounds for an adjustment to the construction period or contract value whatsoever.
Clause 11.6 - Environmental disturbance
Controlling all forms of pollution The contractor shall be responsible for and take all precautions in controlling by whatever means necessary all forms of pollution emanating from the site during the construction period due inter alia to noise, artificial light, wind-blown sand, dust, deposits of mud, etc
The contractor is to ensure that all roads which border the site and are used by the contractor during the execution of the works are kept clean and free of any dirt or debris caused by the execution of the works
C.1 - Special Conditions of Contract Refer to C1.2.2 Special Conditions of Contract elsewhere in the tender document which shall be deemed to be incorporated in the tender document.

C TENDER CLOSING

Tender closing date	As Per Tender Notice & Invitation T1.1		Time	As Per Tender Notice & Invitation T1.1
Tender submission address	As Per Tender Notice & Invitation T1.1			
Tender may be submitted by e-mail	Yes/ no?	No	Email address	Not Applicable

C1.2.3 PRINCIPAL BUILDING AGREEMENT CONTRACT DATA (CONTINUED)**D TENDERER'S SELECTION (to be completed by the tenderer)****D 1.0 Securities [11.0]**Guarantee for construction: Select Option A or B ☐

Option A	Guarantee for construction (variable) by contractor [11.1.1]		
Option B	Guarantee for construction (fixed) by contractor [11.1.2]		
Guarantee for payment by employer [11.5.1; 11.10]	Amount	Not Applicable	
Advance payment, subject to a guarantee for advance payment [11.2.2; 11.3]	Amount	TBC	

D 2.0 Contractor's annual holiday periods during the construction period

Year 1 contractor's annual holiday period	Start date	19 Dec 2025	End date	05 Jan 2026
Year 2 contractor's annual holiday period	Start date	18 Dec 2026	End date	04 Jan 2027
Year 3 contractor's annual holiday period	Start date	N/A	End date	N/A

D 3.0 Payment of Preliminaries [25.0]

Select Option A or B ☐ Where the contractor does not select an option, Option A shall apply

Where the total amount of preliminaries is not identified (in a lump sum contract) it shall be taken as 7.5% (seven and a half percent) of the contract sum, excluding contingency sums and any provision for contract price adjustment (cost fluctuation)

Option A	Assessed by principal agent, an amount pro-rated to the value of the works executed in the same ratio as the amount of the preliminaries to the contract sum which contract sum shall exclude the amount of preliminaries. Contingency sum(s) and any provision for contract price adjustment (cost fluctuations) shall be excluded for the calculation of the aforesaid ratio.
Option B	An amount agreed by the principal agent and the contractor in terms of the bills of quantities or the priced document to identify an initial establishment charge, a time-based charge and a final disestablishment charge. Payment of the time-based charge shall be adjusted from time to time as may be necessary to take into account the progress of the works.

C1.2.3 PRINCIPAL BUILDING AGREEMENT CONTRACT DATA (CONTINUED)**D 4.0 Adjustment of Preliminaries [26.9.4]**

Select Option A or B ☐ Where the contractor does not select an option, Option A shall apply

The amount of preliminaries shall be adjusted to take account of the effect of changes in time and/or value on preliminaries. Such adjustment shall be based on the particulars provided by the contractor for this purpose in terms of Option A or B, shall preclude any further adjustment of the amount of preliminaries and shall apply notwithstanding the actual employment of resources by the contractor in the execution of the works.

For the adjustment of preliminaries both the contract sum and the contract value shall exclude the amount of preliminaries, all contingency sum(s) and any provision for Cost Price Adjustment (cost fluctuations).

Where the total amount of preliminaries is not identified (in a lump sum contract) it shall be taken AS 7.5% (seven and a half percent) of the contract sum, excluding contingency sums, and any provision for contract price adjustment (cost fluctuation).

D TENDERER'S SELECTION (CONTINUED)

Option A	The preliminaries shall be adjusted in accordance with an allocation of preliminaries amounts to be provided by the contractor within fifteen (15) working days of the date of acceptance of the tender as follows: - An amount which shall not be varied; - An amount varied in proportion to the contract value as compared to the contract sum; - An amount varied in proportion to the number of calendar days extension to the date of practical completion to which the contractor is entitled with an adjustment of the contract value as compared to the number of calendar days in the initial construction period. Where the above-mentioned information is not provided the following allocation of preliminaries amounts shall apply: - ten percent (10%) shall not be varied - fifteen percent (15%) shall be varied in proportion to the contract value as compared to the contract sum - seventy-five percent (75%) shall be varied in proportion to the number of calendar days extension to the date of practical completion to which the contractor is entitled with an adjustment of the contract value as compared to the number of calendar days in the initial construction period Where completion in sections is required the contractor shall provide an apportionment of preliminaries per section. Should the contractor fail to provide the apportionment of the preliminaries per section the categorised amounts shall be prorated to the cost of each section within the contract sum as determined by the principal agent.
Option B	The preliminaries shall be adjusted with a detailed breakdown of preliminaries amounts for the works or of a section to be provided by the contractor within fifteen (15) working days of possession of the site. Such breakdown shall inter alia include administrative and supervisory staff charges for the use of construction equipment, all in terms of the programme. The adjustment of preliminaries shall be based on the number of calendar days extension to the date of practical completion to which the contractor is entitled with an adjustment of the contract value as compared to the number of calendar days in the initial construction period taking into account the resources planned for the period of construction during which the delay occurred (not for the period added to the initial or extended date for practical completion).

	Where the contractor does not provide the detailed breakdown of preliminaries within the period stated, Option A shall apply.
--	---

DEPARTMENT OF TRADE AND INDUSTRY

DTI - MAIN CAMPUS

INSTALLATION**REV 0A**

17 Oct 2025

SUMMARY**COST SUMMARY**

ITEM	DESCRIPTION	TOTAL
1	SCHEDULE 1 - PRELIMINARY & GENERAL	
2	SCHEDULE 2 - CIVIL & ELECTRICAL	
3	SCHEDULE 3 - CONTROL ROOM	
4	SCHEDULE 4 - ACCESS CONTROL	
4	SCHEDULE 5 - IP SURVEILLANCE	
WORKS TOTAL (excl. VAT):		
VAT (@ 15%):		
WORKS TOTAL (incl. VAT):		

DEPARTMENT OF TRADE AND INDUSTRY					
DTI - MAIN CAMPUS					
SCHEDULE 1 - PRELIMINARY AND GENERAL					
SUBTOTAL FOR SCHEDULE 1 - PRELIMINARY AND GENERAL - CARRIED TO SUMMARY					
ITEM	DESCRIPTION	UNIT	RATE		
1.1	Mark-up percentage on any non-scheduled items (PC SUMs).	%			
ITEM	DESCRIPTION	UNIT	QTY	RATE	TOTAL
1.2	Site Establishment (Refer item 11.3 detailed scope of works)	SUM	1		
1.3	Insurance	SUM	1		
1.4	Security	SUM	1		
1.5	Travelling	SUM	1		
1.6	Telephone	SUM	1		
1.7	Guarantees (Contractors Guarantee)	SUM	1		
1.8	Others (Specify)	SUM	1		
1.9	Total Mark-up at the stated percentage for any non-scheduled items (PC SUMs).	SUM	1		
1.10	Total sum for all consumables required for this contract.	SUM	1		
SUBTOTAL FOR SCHEDULE 1 - PRELIMINARY AND GENERAL - CARRIED TO SUMMARY					R -

DEPARTMENT OF TRADE AND INDUSTRY

DTI - MAIN CAMPUS

SCHEDULE 2 - CIVIL AND ELECTRICAL

SUBTOTAL FOR SCHEDULE 2 - CIVIL AND ELECTRICAL - CARRIED TO SUMMARY

R

-

ITEM	DESCRIPTION	UNIT	QTY	SUPPLY	INSTALL	RATE	TOTAL
2.1	TRUNKING, CABLE TRAYS, AND SLEEVES						
2.1.1	SABS approved P9000 trunking, <u>including</u> all adapters, couplings, t-pieces, splits, bends, forks, corners, fastnings, brackets, screws, covers, anchors, suspenders, and any miscellaneous items required to make the installation complete, <u>resolved to a per meter rate</u> . <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	m	Rate				
2.1.2	SABS approved P2000 trunking, <u>including</u> all adapters, couplings, t-pieces, splits, bends, forks, corners, fastnings, brackets, screws, covers, anchors, suspenders, and any miscellaneous items required to make the installation complete, <u>resolved to a per meter rate</u> . <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	m	1000				
2.2	PVC CONDUITS						
2.2.1	SABS approved conduit PVC - 25mm, <u>resolved to a per meter rate</u> . The <u>rate must account for any and all</u> adapters, couplings, t-pieces, splits, bends, forks, fastnings, brackets, screws, <u>Sprague</u> , and any miscellaneous items that may be required to complete a typical cable route and make the installation complete <u>with a spacerbar saddle every 1m</u> . <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	m	Rate				
2.2.2	SABS approved conduit PVC - 20mm, <u>resolved to a per meter rate</u> . The <u>rate must account for any and all</u> adapters, couplings, t-pieces, splits, bends, forks, fastnings, brackets, screws, <u>Sprague</u> , and any miscellaneous items that may be required to complete a typical cable route and make the installation complete <u>with a spacerbar saddle every 1m</u> . <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	m	1000				

DEPARTMENT OF TRADE AND INDUSTRY

DTI - MAIN CAMPUS

SCHEDULE 2 - CIVIL AND ELECTRICAL

SUBTOTAL FOR SCHEDULE 2 - CIVIL AND ELECTRICAL - CARRIED TO SUMMARY

R

-

ITEM	DESCRIPTION	UNIT	QTY	SUPPLY	INSTALL	RATE	TOTAL
2.3	SPARE FITTINGS						
2.3.1	SABS approved Steel 2 x 4 box recessed - <u>including</u> screws, and any miscellaneous items required to make the installation complete. [Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.] (Supplied, Installed, Tested, and Commissioned).	EA	Rate				
2.3.2	SABS approved PVC 2 x 4 box surface mount - <u>including</u> screws, and any miscellaneous items required to make the installation complete. [Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.] (Supplied, Installed, Tested, and Commissioned).	EA	Rate				
2.4	ELECTRICAL WORKS						
2.5.1	15 kVA Online double conversion 3 phase UPS N + 1. Lithium Ion Batteries [Including all sundries required to make the fitting complete and the installation functional and compliant to the satisfaction of the Engineer and the Client.]	EA	1				
SUBTOTAL FOR SCHEDULE 2 - CIVIL AND ELECTRICAL - CARRIED TO SUMMARY							R -

DEPARTMENT OF TRADE AND INDUSTRY DTI - MAIN CAMPUS							
SCHEDULE 3 - CONTROL ROOM UPGRADE							
ITEM	DESCRIPTION	UNIT	QTY	SUPPLY	INSTALL	RATE	TOTAL
3.1	MONITORS AND BRACKETS						
3.1.1	55 Inch-LED 0.88 IMAGE TO IMAGE (Item 4.3.1 in detail scope of works) <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	10				
3.1.2	BRACKET – PUSH IN POP OUT HYDRAULIC TYPE (Item 4.3.2) in detail scope of works) <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	10				
3.1.3	24 Inch Full HD Monitors <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	12				
3.2	CONTROLLERS AND PERIPHERALS						
3.2.1	8x12HDMI 8 input 20 output videowall controller (Item 4.3.3) in detail scope of works) <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	1				
3.2.2	Fibre Optic HDMI Cables 30 m lengths <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	12				
3.3	SERVER AND OPERATOR WORKSTATION						
3.3.1	Integration Server - Ironlink 4 Bay Rackmount server standard with 7.2TB usable storage Keyboard and mouse included. <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	1				
3.3.1	Control Room Desk capable of housing four(4) 24 Inch monitors including brackets - Comfortio Operator desk system of similar <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	3				
3.3.2	Control room operator chair (Item 4.5 in detailed scope of works) <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	3				
3.3.3	Access Control Workstation - I7 processor, 16 GB RAM, 500 SSD, Quad Display <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	Ea	4				
3.4	RAISED FLOOR, RENEVATIONS						
3.4.1	Raised floor for both the equipment room and control room (Item 4.2 in detailed scope of works) <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	m ²	50				
3.4.2	Renervations of the existing space <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	PC Sum	1	R 250 000.00	R -	R -	R 250 000.00
SUB TOTAL FOR SCHEDULE 3 - CONTROL ROOM UPGRADE - CARRIED FORWARD						R	250 000.00

DEPARTMENT OF TRADE AND INDUSTRY
DTI - MAIN CAMPUS

SCHEDULE 4 - ACCESS CONTROL SYSTEM

ITEM	DESCRIPTION	UNIT	QTY	SUPPLY	INSTALL	RATE	TOTAL
4.1	CONTROLLERS						
4.1.1	CONTROLLER 7000 STANDARD <u>including all power supplies, backup batteries, terminations, brackets, fixing materials,</u> connections and interfacing to reader module(s), and all other accessories to make the installation complete. The controller must be able to function offline. <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	51				
4.1.2	Gallagher OSDP 8 Port Hub <u>including all</u> terminations, mounting plates, brackets, <u>fixing materials,</u> connections and hardware interfacing, and all other accessories to make the installation complete. <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	2				
4.1.3	8 HBUS module - including all terminations, brackets, fixing materials, and all other accessories to make the installation complete. <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	21				
4.1.4	HBUS 8 in 4 out door module - including all terminations, brackets, fixing materials, and all other accessories to make the installation complete. <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	10				
4.1.5	Controller 6000 I/O Mounting Plate including all terminations, brackets, fixing materials, and all other accessories to make the installation complete. <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	51				
4.1.6	OSDP 8 Port hub including all terminations, brackets, fixing materials, and all other accessories to make the installation complete. <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	51				
4.2	CONTROLLER CABINETS AND READERS						
4.2.1	Secure controller dual housing cabinet including 8A PSU, complete with mounting plates, tamper boards, spacers, fuse boards, wire fasteners and cable anti-strain measures to house controllers, modules and expansion boards, etc., including all brackets, <u>fuses,</u> and other accessories to make the installation complete. <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	51				
4.2.2	Push-to-Exit (no-touch) sensors. <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	5				
4.2.3	T15 MULTI TECH READER BLACK Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.] (Supplied, Installed, Tested, and Commissioned)	EA	472				
4.2.4	MIFARE DESFIRE ISO CARD 4K EV3 Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.] (Supplied, Installed, Tested, and Commissioned)	EA	1 000				
4.3	BIOMETRIC READERS AND ENROLMENT						
4.3.1	MORPHO SIGMA LITE MULTI (BIO+CARD+LED), complete with sundries required to make the fitting complete and the installation functional and compliant <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	4				

DEPARTMENT OF TRADE AND INDUSTRY
DTI - MAIN CAMPUS

SCHEDULE 4 - ACCESS CONTROL SYSTEM

ITEM	DESCRIPTION	UNIT	QTY	SUPPLY	INSTALL	RATE	TOTAL
4.3.2	Take-On Reader for Biometrics – FINGERPRINT, USB, complete with all brackets and other accessories to make the installation complete. <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	1				
4.4	MAGNETIC AND ELECTRO-MECHANICAL LOCKS						
4.4.1	Magnetic Lock <u>300kg</u> : Standard Surface Mount, <u>Unmonitored</u> , complete with all brackets and mounting accessories. <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	204				
4.5	BREAKGLASS UNITS						
4.5.1	BREAK GLASS TYPE 1 – ACCESS CONTROL : GREEN over-ride unit (No backbox), <u>resettable</u> . <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	204				
4.5.2	BREAK GLASS LENSES TYPE 1 – ACCESS CONTROL : GREEN RESETTABLE PLASTIC. <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	204				
4.6	NETWORK EQUIPMENT						
4.6.1	UniFi Pro 24 - Port Switch with 2 GBIC PORTS <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	18				
4.6.2	Twenty Four (24) Way 19" CAT-6 Patch Panel [Krone 24 port CAT6 patch panel] <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	Rate				
4.6.3	Patch lead 1 m <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	Rate				
4.7	DOOR POSITION SWITCHES						
4.7.1	Door Position Switch Type 1 - Flush Mount complete with all accessories. <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	204				
4.8	KEY-OVERRIDES AND OVERRIDE PUSH-BUTTONS						
4.8.1	Key-Override KS1 - Standard key-override fitted with <u>security torx screws</u> and secured with <u>loctite threadlocking</u> . <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	35				
4.8.2	Key-override KS2 - High Security Key-Override. <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	Rate				
4.9	STAINLESS STEEL BACK PLATES						
4.9.1	Stainless Steel Back Plate (280mm x 280mm x 2mm) for Intercom / Breakglass / Proximity / Biometric Reader / Push-to-Exit as per the Engineer's design. <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	408				
4.10	WIRING AND CONNECTORS						
4.10.1	Mylar cable 0.22mm ² x 8 core. <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	m	10 000				

DEPARTMENT OF TRADE AND INDUSTRY
DTI - MAIN CAMPUS

SCHEDULE 4 - ACCESS CONTROL SYSTEM

ITEM	DESCRIPTION	UNIT	QTY	SUPPLY	INSTALL	RATE	TOTAL
4.10.2	Mylar cable 0.5mm ² x 4 core. <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	m	Rate				
4.10.3	<u>CAT-6 UTP Cable</u> , (Item 2.3 in Detailed scope of Works) <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	m	10 000				
4.11	DOOR CLOSERS						
4.11.1	Door widths up to 950 mm (TS 91)Door Closers with slide chanel. <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	110				
4.11.2	Geze automatic door closer EMD Slimline EMD-F <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	100				
4.11.3	Flexible Stainless Steel Armored Door Loop with ABS ends •EA-1045 Dimension Length : 393mm Door sensors. <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	205				
4.12	SOFTWARE, CONFIGURATION, TRAINING, MAINTENANCE AND MANUALS						
4.12.1	Software (Command Centre) for all above-mentioned hardware capable of controlling all access controlled doors on the site. <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	SUM	1				
4.12.2	Door License. <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	SUM	246				
4.12.3	Encoder unit <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	SUM	2				
4.12.4	Workstation license . <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	SUM	6				
4.12.5	Photo ID and encoding License. <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	SUM	1				
4.12.6	IDEMIA MSO330 WITH VERIF LICENSE BUNDLE <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	SUM	1				
4.12.7	System Configuration and integration with the following systems • BMS (Tridium) • IP Surveillance (Cathexis) • PA System (TOA) • Intercom (Commax) • Intruder detection system (DSC) • Electronic Key Management System <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	SUM	1				

DEPARTMENT OF TRADE AND INDUSTRY
DTI - MAIN CAMPUS

SCHEDULE 4 - ACCESS CONTROL SYSTEM

ITEM	DESCRIPTION	UNIT	QTY	SUPPLY	INSTALL	RATE	TOTAL
4.12.8	Rest API view alarms and events (Cathexis) <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	1				
4.12.9	Video Viewer SDK (Cathexis) <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	1				
4.12.10	BACNET Base license (Tridium) <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	1				
4.12.11	BACNET object license (Tridium) <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	200				
4.12.12	SIP Integration license (TOA) <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	1				
4.12.13	SIP Device license (TOA) <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	20				
4.12.14	Traka license (Key Management) <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	1				
4.12.15	Kone and Schindler ELI license (Lifts) <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	1				
4.12.16	Rest API View Status license <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	1				
4.12.17	Rest API Override license <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	1				
4.12.18	Rest API create events and alarms <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	1				
4.12.19	Integration Server - Ironlink 4 Bay Rackmount server standard with 7.2TB usable storage Keyboard and mouse included. <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	1				
4.13	CARE PACKAGE SOFTWARE AND LICENSING						
4.13.1	Door License SMA. <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	SUM	246				
4.13.2	Workstation license SMA <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	SUM	6				

DEPARTMENT OF TRADE AND INDUSTRY							
DTI - MAIN CAMPUS							
SCHEDULE 4 - ACCESS CONTROL SYSTEM							
ITEM	DESCRIPTION	UNIT	QTY	SUPPLY	INSTALL	RATE	TOTAL
4.13.3	Rest API view alarms and events SMA <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	1				
4.13.4	Video Viewer SDK SMA <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	1				
4.13.5	BACNET Base license SMA <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	1				
4.13.6	BACNET object license SMA <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	200				
4.13.7	Visitor management self reg kiosk <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	1				
4.13.8	SIP Integration license SMA <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	1				
4.13.9	SIP Device license SMA <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	1				
4.13.10	Traka license SMA <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	1				
4.13.11	Kone and Schindler ELI license SMA <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	1				
4.13.12	Rest API Override SMA <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	1				
4.13.13	Rest API create events and alarms SMA <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	1				
4.13.14	Rest API cardholders SMA <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	1				
4.14	MAINTENANCE						
4.14.1	12-months of Maintenance coinciding with the guarantee/warranty period for the equipment (5 callouts per month included).	SUM	1				
4.14.2	Additional callouts over and above what is included in the 12-months Maintenance coinciding with the guarantee/warranty period. Per callout.	EA	1				
SUB TOTAL FOR SCHEDULE 4 - ACCESS CONTROL SYSTEM - CARRIED FORWARD						R	-

DEPARTMENT OF TRADE AND INDUSTRY							
DTI - MAIN CAMPUS							
SCHEDULE 5 - CCTV							
SUBTOTAL FOR SCHEDULE 5 - CCTV - CARRIED TO SUMMARY							
ITEM	DESCRIPTION	UNIT	QTY	SUPPLY	INSTALL	RATE	TOTAL
5.1	CAMERAS						
5.1.1	Axis P1467-LE Bullet camera <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA					
5.1.2	Axis M4216-V 4MP Dome camera <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	152				
5.2	NETWORK POINTS						
5.2.1	CAT-6 UTP (Item 2.3 in Detailed scope of Works) <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	m	9120				
5.5	SERVERS, STORAGE, SORFTWARE						
5.5.1	CATHEXIS WINDOWS NVR3000 120TB STD <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	2				
5.5.2	Cathexis Premium License <i>[Including all sundries required to make the fitting complete and the installation functional and compliant to the requirements of the Engineer and the Client.]</i> (Supplied, Installed, Tested, and Commissioned).	EA	152				
5.5	TESTING AND COMMISIONING						
5.5.1	Testing, Adjusting and Commissioning of all the CCTVs per SANS 10222-5-1-4 including supplier support for configuration and setup.	SUM	1				
5.6	SPARES AND LABELLING						
5.6.1	Terminations, Connectors & Labels for all the above mentioned hardware (Supplied, Installed, Tested and Commissioned).	SUM	1				
SUBTOTAL FOR SCHEDULE 5 - CCTV - CARRIED TO SUMMARY							R -

DETAILED SCOPE OF WORKS – DTI MAIN CAMPUS ISMS AND CONTROL ROOM UPGRADE

PREPARED BY : Steyn de Lange

DATE : 08 December 2025

TABLE OF CONTENTS

1. PROJECT OVERVIEW	2
1.1. Campus layout and project implementation.....	2
1.1.1. Campus Layout	2
1.1.2. Project Implementation and current ISMS on campus	2
1.1.3. Site Establishment.....	2
2. EQUIPMENT	2
2.1. Hardware Removal	2
2.2. Hardware installation	3
2.2.1. General	3
2.3. Cabling.....	3
3. HEAD END INSTALLATION	3
3.1. Centralized control room.....	3
3.2. Software.....	3
3.3. Licensing.....	4
3.4. ISMS Integration	4
4. CONTROL ROOM UPGRADE	5
4.1. Control room entrance	5
4.2. Raised Floor.....	5
4.2.1. Scope.....	5
4.2.2. General	6
4.2.3. Specification	6
4.3. Video Walls	6
4.3.1. 55 Inch narrow bezel monitors.....	6
4.3.2. Push in pop out hydraulic brackets.....	7
4.3.3. Video Wall Controller	7
4.4. Operator workstations	7
4.5. Operator Chairs	7
5. TRAINING.....	8
5.1. General	8
5.2. Operator Training.....	8
6. HANDOVER	8
6.1. Close Out documentation	8
6.2. As-Built Drawings and schematic diagrams.....	9
7. MAINTENANCE	9
7.1. General Maintenance.....	9
7.2. Guarantee and Maintenance Period.....	10

1. PROJECT OVERVIEW

1.1. CAMPUS LAYOUT AND PROJECT IMPLEMENTATION

1.1.1. CAMPUS LAYOUT

The campus consists of the following Blocks:

- Block A
- Block B
- Block C
- Block D
- Block E
- Block F
- Block SSC
- Basement level 1
- Basement level 2

1.1.2. PROJECT IMPLEMENTATION AND CURRENT ISMS ON CAMPUS

The project scope will be implemented in all the blocks except for Block B. The project will be implemented in stages one block at a time. The current system utilized on site as the ISMS (Integrated Security Management System) is the Gallagher system.

An alternative to the Gallagher system shall be considered should it meet the requirements in the specification documentation as well as the scope of works as intended. The proposed alternative should also be able to integrate the existing Gallagher system.

1.1.3. SITE ESTABLISHMENT

Due to the phased approach of the security upgrade, the successful bidder would need to bring equipment onto site as and when it is required. Should a more permanent site camp/office be required, this could be negotiated with the client. It must be noted that the campus is still a functional campus with limited space available.

These conditions must be noted when consideration for pricing is completed in the preliminary and general section of the BOQ.

2. EQUIPMENT

2.1. HARDWARE REMOVAL

The following hardware needs to be removed from all the Blocks on the DTI campus:

- Babylon access controllers
- Wooden backing plates
- Intercom units
- Green Break glass units
- Babylon Proximity card readers
- Existing biometric readers
- Automated doors closers
- Manual door closers

An inventory of the removed equipment is to be documented per building per floor. The equipment needs to be stored in an area to be identified by the client.

2.2. HARDWARE INSTALLATION

2.2.1. GENERAL

The hardware installation is as follows:

- Gallagher controllers (or similar) replacing the Babylon controllers
- Stainless Steel backing plates replacing the wooden plates
- Removed intercom units to re-installed in original positions
- New green break glass units to replace the removed ones
- Gallagher T15 (or similar) units to replace the Babylon card readers
- Sagem Sigma biometric readers to replace the existing readers
- Geze automated door closers to replace the existing door closers
- T91 manual door closers to replace existing

Several items are a like for like replacement, whilst others are either an upgrade of the existing equipment on site

2.3. CABLING

The existing Mylar cable is to be retained as far as possible. The cables need to be tested by the contractor for any degradation and replaced where necessary. Should any additional cabling be required, this would need to be confirmed with the security consultant.

The existing CAT 5 cable will need to be replaced with the CAT 6 cable as per the bill of quantities. The CAT-6 Cabling shall be used for all Ethernet Connections within buildings or other approved short haul distances. The cable shall provide performance of up to 250 MHz and be suitable for 10BASE-T, 100BASE-TX (Fast Ethernet), 1000BASE-T/1000BASE-TX (Gigabit Ethernet) and 10GBASE-T (10-Gigabit Ethernet).

22 to 24 AWG copper is allowed if the ANSI/TIA-568-B.2-1 performance specifications are met. Cat 6 patch cables are normally terminated in 8P8C (RJ-45) modular connectors.

3. HEAD END INSTALLATION

3.1. CENTRALIZED CONTROL ROOM

There is an existing centralized control room situated in the basement level 1. This control room will be the main control room for the entire campus. The main integration server will be installed in the equipment room adjacent to the control room.

The project is going to be implemented in a phased manner one block at a time. There will be no sub-servers installed per block as the centralized control room will accommodate the entire campus with each block being brought online as the project progresses.

3.2. SOFTWARE

The ISMS (Integrated Security Management System) will be the sole platform with various modules for all integrations on the campus. One of the modules is the access control system module that replace the existing Babylon access control system. The ISMS access control module must be installed with the following items being setup/programmed:

-
- Set up test environment
 - Outline system architecture
 - Data exchange using Rest API
 - Test and ensure that both card technologies are functional on the new and existing systems
 - New door Configuration
 - Set up access groups
 - Convert the SQL database
 - Migrate entire Babylon access database (Staff, contractors, etc.)
 - Ensure that the supplier is actively involved in the entire process

3.3. LICENSING

The contractor shall ensure that all door and workstation licenses are installed and tested. Proof of licensing is to be provided and handed over to the client in the hand over files.

The licenses provided should be a once off cost with access to the latest firmware updates and support for the first 12 months. The option to extend the license period to obtain the latest firmware updates may be done at the client's discretion. The decision to not extend the license should not impact the functionality of the system.

3.4. ISMS INTEGRATION

The purpose of the ISMS system is to integrate all electronic systems on campus onto a singular platform. GUI's (Graphical user interfaces) will be required per block as per the specification to process events and popups on the preconfigured operator dashboards.

The contractor shall ensure that the ISMS is integrated with the following sub-systems/modules:

- BMS (Building Management System)
- IP Surveillance system
- Fire Suppression system
- Fire detection systems
- Intruder detection systems
- IP Intercoms
- Vertical transportation systems
- PA System
- Electronic Key Management system

A BMS annexure document forms part of the tender documentation indicating the type and quantity of items to be integrated and made available on the GUI's to be monitored and interacted with.

The IP surveillance system on campus consists of 316 IP surveillance cameras which will be utilized to popup on events in all areas of the campus specific to that event.

The events that will require video popups are as follows but not limited to:

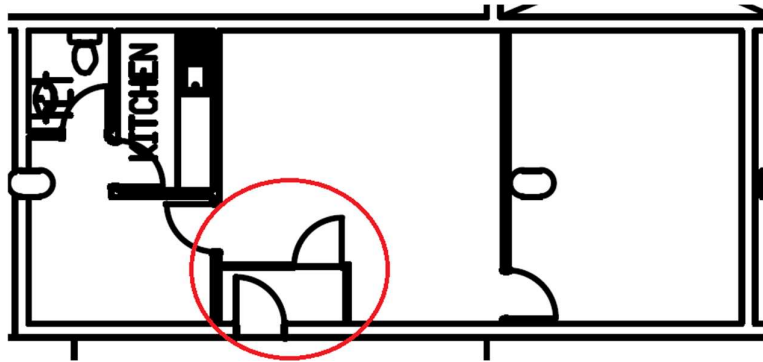
- Access control events e.g. Break glass broken, door forced, anti-pass back violation
- Fire alarms
- Intruder alarms

- BMS critical alarms e.g. Electrical events, Vertical transportation events, HVAC events

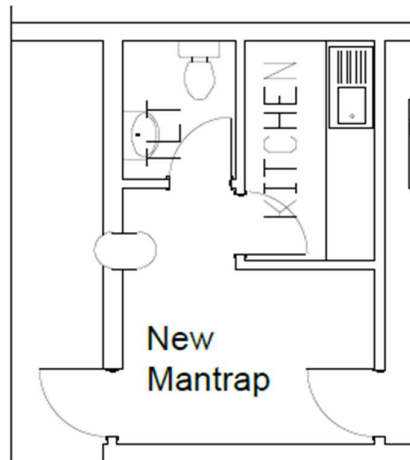
4. CONTROL ROOM UPGRADE

4.1. CONTROL ROOM ENTRANCE

The existing entrance (mantrap) to the control room needs to be removed with the outer door removed and bricked up.



A new entrance needs to be installed in the left side wall to be used in conjunction with the interleading door from the kitchen and ablution facilities to form the new mantrap entrance. The doors must operate as interlocking doors.



4.2. RAISED FLOOR

4.2.1. SCOPE

This section deals with raised access floor systems supported off the structural floor to form a void for the distribution of services. The construction normally consists of panels supported on a grid of pedestals which have a vertical height adjustment mechanism.

Access to the void is through removable panels.

Flooring System to Method of Build Performance Spec MOB PF2 PS/SPU (March 1992) unless specified otherwise.

4.2.2. GENERAL

- It shall be an anti-static raised floor system that will ensure ease of reticulation within the room as well as accommodating the air conditioning / ventilation to the equipment inside the room.
- Floor void is to be a minimum of 300mm deep.
- Cable openings are to be provided with sufficient cable protection covers.
- Cable trays shall be provided under the raised floor. This will ensure that if a water leak occurs in the area the cables will not be lying in the water.

4.2.3. SPECIFICATION

- Subfloor: Fine to medium tamped finish. Power floated finish is NON-PREFERRED.
- Preparation: Floor to be thoroughly swept to remove all loose dust and debris and two coats of PVA floor sealer applied prior to laying pedestals.
- Access Type: Full
- Strength Grade: Heavy
- Point Load 25mm x 25mm 4.5kN
- Uniform Distributed Load 12kN/m²
- All values will withstand a safety factor of 3
- CEN References 6A Heavy
- CISCA References 2500LBS
- System Weight 46kg/m² inclusive of pedestals at 150mm FFH.
- Panels shall be 600mm square and shall be interchangeable with other panels except where cut for special purposes. Panels shall be easily removed and replaced without disturbing adjacent panels, by one person using a portable lifting device.
- Panels shall be protected from corrosion by the manufacturer's standard factory applied finishes.
- Under structure type shall be selected from the standard range with due regard to height and loading criteria and shall be protected from corrosion using galvanized or nonferrous materials in its construction.
- Pedestal Grid Centres 600mm
- Finished floor height above subfloor (nominal): 300 mm.

4.3. VIDEO WALLS

Two video walls are to be installed in the control room consisting of push-out monitor brackets housing 55-inch narrow bezel monitors. The configuration of the video walls are as follows:

- 3 x 2 video wall
- 2 x 2 video wall

A video wall controller will be installed with adequate functionality to enable video to be pushed between the video walls and operator workstations.

4.3.1. 55 INCH NARROW BEZEL MONITORS

The monitors must comply with the following specifications:

- Aspect Ratio – 16:9
- Display Color – 16.7M
- Brightness – 500cd/m²

-
- Contrast – 1100:1
 - Response Time – 5ms
 - Seam – 0.88mm
 - Compatible HD/SD and HDMI Input - 400i/P, 576i/P, 720P, 1080i/1080P

4.3.2. PUSH IN POP OUT HYDRAULIC BRACKETS

The brackets must comply with the following specifications:

- Compatible Screen Size: 55 Inch
- Weight Capacity: 100kgs
- Pop-Out Extension Depth: Up to 200mm (8")
- VESA Mounting Patterns: 400x400mm to 600x400mm, with a maximum horizontal extension up to 700mm
- Hydraulics: heavy-duty hydraulic rods

4.3.3. VIDEO WALL CONTROLLER

The controller must comply with the following specifications:

- Signal Acquisition - •VGA, DVI, HDMI, CVBS, DP, Dual-Link DVI SDI, HDBaseT, IP-Video, Fiber
- Customized resolution - •800x600, 1366x768, 1400x900, 1920x1080, 4K
- Control – RS232, Network, Key Button, Remote control
- MTBF - > 50 000 hrs
- Input resolution - 3840x2160@60Hz
- Output resolution - 3840x2160@30Hz

4.4. OPERATOR WORKSTATIONS

Three operator workstations are to be installed in the control room. Each workstation must have four 24-inch monitors installed on it. Each monitor will display a different Gallagher command centre dashboard. The dashboards will be as follows:

- Alarm Viewer
- IP Surveillance event displays
- GUI event pop-ups
- Custom for operator (Playbacks, scrolling, etc.)

4.5. OPERATOR CHAIRS

The operator chairs must meet the following specification:

- 500 000 Martindale scoring
- Seat mechanism - torsional spring, easily adjustable for weights from 45 kg to 150 kg (99 lbs - 330 lbs), statically loadable up to 200 kg (440 lbs), can be tilted and locked at any angle: - 6° to +19°.
- Pneumatic lumbar support, Adjustable
- Cushioning - Ergonomically shaped cold foam
- Height adjustment: Gas Spring, adjustable to any height from 44 - 56 cm
- 6-legged base design

5. TRAINING

5.1. GENERAL

Prior to commissioning of the installation, the contractor shall provide comprehensive training of all security staff and nominated maintenance personnel, to the approval of the Engineer and the CLIENT.

Maintenance staff shall demonstrate a complete understanding of the location and connectivity of the various elements of the security services installation. All training aids and course notes necessary to conduct effective operational and maintenance training shall be supplied by the contractor. The training venue will be made available on Site by the CLIENT.

The training documentation must be submitted to the Engineer for evaluation and approval. No training will commence on site prior to the written approval of the Engineer. Should the Engineer not approve the drawings all documentation will be referred to the Contractor for re-evaluation and submission to the Engineer.

Documentation must be sent to the Engineer at least 12 working days prior commencement or scheduling of training programs of the operational staff on site.

5.2. OPERATOR TRAINING

Training shall be comprehensive, covering all aspects of systems installed as part of these works.

The contractor shall provide a detailed training program to the Engineer, for comment and review, no less than 12 days prior to the commencement of training.

Training shall be adequate to ensure that the groups trained are :

- competent in the operation of systems,
- adequately trained to carry out ongoing training,
- fully aware of the location of all equipment installed as part of this Contract within their area of responsibility.

Full training of the System Operators (All security staff) must be included in the tender.

6. HANDOVER

6.1. CLOSE OUT DOCUMENTATION

The tenderer shall note that after the completion of the contract three sets of all operating, maintenance and training manuals as well as a complete spares list for all the equipment and software installed (together with two local agency telephone numbers where the above can be obtained), shall be handed to CLIENT.

The tenderer shall at the end of the contract update all the drawings that were issued to him during the contract with a red pen and hand them over to the engineer for finalization and completion of his contractual obligation regarding drawings.

All the above shall form part of the as-built documentation.

The retention payable as per the agreement with the CLIENT after the completion of the as-built documentation shall only be payable once all the above has been handed over to CLIENT.

All the required documentation shall be to the satisfaction of the Engineer and of the CLIENT.

6.2. AS-BUILT DRAWINGS AND SCHEMATIC DIAGRAMS

- (a) The Engineer's drawings for the Contract shall be those issued at the times of tender together with any others issued to cover the variations to the Contract. These drawings must be processed by the contractor and any queries submitted within two (2) weeks.
- (b) As part of this Contract the Contractor shall provide the following Drawings:
 - Manufacturing and Installation Drawings:
 - The manufacturing and installation drawings ("shop drawings") shall provide all details of the components necessary for the manufacture and installation of the system in accordance with the specification.
 - Wiring Diagrams:
 - The wiring diagrams shall provide details of all the wiring associated with the installation.
 - The same drawing symbols and system shall be used, as used on the Engineer's Drawings.
 - Builder's Work Drawings:
 - All necessary builders' work drawings, as described elsewhere in this specification, shall be provided as part of this Contract.
 - AS BUILT Drawings:
 - On completion of the installation, but before the plant is handed over; the Contractor shall provide a complete set of drawings showing the completed installation including wiring.
 - In addition to the drawings listed above, the Contractor shall provide all drawings necessary for the execution of the Contract and shall submit such general and detailed drawings of the components and apparatus, as the Engineer may require approving construction of the system.
 - Details and drawings of all major items of equipment, made by the Contractor or his suppliers, shall be submitted for approval without specific request from the Engineer.
 - All required drawings shall be submitted to an agreed program to suit the construction of the system.
 - All drawings shall be clearly numbered or marked with the equipment item numbers, area references etc.

7. MAINTENANCE

7.1. GENERAL MAINTENANCE

Maintenance of the specified systems, services and/or parts of buildings and infrastructure shall all be referred to as "Maintenance of the Installation".

Maintenance of the completed installation shall ensure the reliable functioning and optimum service life thereof.

Maintenance of the installation shall commence upon the completion of the installation contract, and the successful handover to the client, and continue for a period of 12-months. (The appointment of the sub-contractor for the 12-month maintenance period shall be to the discretion of the client.

The price submitted herein shall remain an option for implementation to the full discretion of the Client, that may opt to go out on a public tender for this maintenance of the security installation should they wish to do so.

The monthly maintenance responsibilities of the installation include all units and components as specified herein.

The maintenance of the installation shall be performed in accordance with the Technical and Particular Specifications, the Operating and Maintenance Manuals and the Maintenance Control Plan.

Remuneration for maintaining the installation (systems, services and/or buildings and parts of the infrastructure) in perfect functional condition is provided for in the Schedules of Quantities by means of monthly payment items.

This Additional Specification covers maintenance requirements, development of a maintenance control plan, identification of equipment, site maintenance administration, maintenance performance measurement, as well as the items for measurement of the Contractor's service level and resulting payment.

7.2. GUARANTEE AND MAINTENANCE PERIOD

The tenderer shall note that a one-year full maintenance period shall be applicable on all aspects of the work done under this contract effective from the date of practical completion.

This shall include full a full back-up service for all the equipment and cabling rendered installed as well as all software installed by the successful tenderer under this contract.

The tenderer shall in his price fully state the monthly charge for the above inclusive of his additional rate for labour for any after hour work required.

DEPARTMENT OF TRADE AND INDUSTRY - ISMS SPECIFICATION

PREPARED BY : Steyn De Lange

DATE : 04 September 2025

TABLE OF CONTENTS

1.	GENERAL	3
2.	RESPONSE FORMAT	3
3.	PRODUCT ACCEPTANCE.....	4
4.	FUNCTIONAL OVERVIEW.....	4
5.	LICENSING	7
6.	SYSTEM REQUIREMENTS.....	7
7.	SYSTEM SERVERS AND WORKSTATION INSTALLATION.....	8
8.	CENTRAL CONTROL AND SYTEM MANAGEMENT SOFTWARE.....	9
9.	COMMUNICATIONS AND DIAGNOSTICS	12
10.	CYBERSECURITY	13
11.	MULTIPLE SERVER CONNECTIVITY	13
12.	GRAPHICAL OPERATOR INTERFACE	14
13.	SYTEM OPERATOR MANAGEMENT	17
14.	CARDHOLDER MANAGEMENT	18
15.	PHOTO BAGDING AND IMAGE MANAGEMENT	21
16.	INTRUDER ALARM SYSTEM.....	23
17.	ALARM MANAGEMENT	25
18.	CLASS 5 ALARM SYSTEM	29
19.	ACCESS CONTROL.....	30
20.	PERSONNEL IDENTIFICATION VERIFICATION	34
21.	SITE PLANS.....	35
22.	GUARD TOURS.....	37
23.	REPORTS.....	39
24.	NOTIFICATIONS.....	42
25.	BULK NOTIFICATIONS.....	42
26.	AUDIT TRAIL	42
27.	MOBILE DEVICE APPLICATION	43
28.	COMPETENCIES.....	47
29.	RANDOM SELECTION.....	48
30.	ELEVATOR CONTROL AND MANAGEMENT	48
31.	CAR PARKING	50
32.	LOCKER SYSTEM.....	51
33.	PRE-PROGRAMMED OVERRIDE MACROS	51
34.	VISITOR MANAGEMENT KIOSK.....	52
35.	DOOR FUNCTIONALITY – CONNECTED TO CONTROLLER.....	54
36.	DOOR FUNCTIONALITY – DATA ON CARD.....	56
37.	DOOR FUNCTIONALITY – WIRELESS CONNECTIVITY.....	58
38.	FIELD HARDWARE – INTELLIGENT FIELD CONTROLLER (IFC).....	59
39.	ENCRYPTED END OF LINE DEVICE – CLASS 5.....	65
40.	ENCRYPTED END OF LINE DEVICES	66
41.	ACCESS CONTROL READERS – MIFARE TECHNOLOGY.....	67
42.	ACCESS CONTROL READERS – MULTI TECHNOLOGY	71

43.	ACCESS CONTROL READERS – LONG RANGE.....	75
44.	READER – BLUETOOTH AND NFC	75
45.	ACCESS CONTROL READERS – BIOMETRIC (FINGERPRINT).....	77
46.	ACCESS CONTROL READERS – BIOMETRIC (CONTACTLESS).....	78
47.	ALARM MANAGEMENT TERMINAL – ACCESS CONTROL.....	79
48.	ALARM MANAGEMENT TERMINAL – PERIMETER.....	81
49.	ACCESS CARDS AND TOKENS.....	83
50.	TOKEN – MIFARE CLASSIC TECHNOLOGY	84
51.	TOKEN – MIFARE PLUS TECHNOLOGY	85
52.	TOKEN – MIFARE DESFIRE TECHNOLOGY	85
53.	CREDENTIAL – BLUETOOTH AND NFC ON MOBILE DEVICE	86
54.	CREDENTIAL - BIOMETRIC.....	87
55.	RS485 FIBRE TRANSCEIVER REQUIREMENTS.....	88
56.	ENERGISED PERIMETER INTRUDER DETECTION - STRUCTURE.....	89
57.	ENERGISED SECURITY FENCE CONTROLLER – STAND ALONE	93
58.	ENERGISED SECURITY FENCE CONTROLLER - NETWORKED.....	95
59.	SYSTEM INTEGRATION.....	97
60.	VIDEO MANAGEMENT SYSTEM INTEGRATION.....	100
61.	REST API.....	101

1. GENERAL

This specification calls for the supply, installation, and commissioning of a complete ISMS in accordance with appropriate local and international standards and the technical and performance criteria set out in this document.

The system is to be supplied with all equipment, hardware, software, cabling, and ancillary services as required to provide an ISMS complete and functional in all respects. The tenderers are to familiarise themselves with all matters related to such requirements and to account for such in the tendered price.

Other security system components not included in this specification shall be fully integrated with this ISMS.

It is the responsibility of the tenderer to obtain clarification of all matters in which doubt exists as to the exact intent of this document or in which a conflict appears to have arisen. Such information must be obtained prior to the closing and lodging of tenders.

The response shall clearly detail all pricing for components, cabling, installation, training, commissioning, setting to work, and a 24-month comprehensive warranty.

The tenderer must include as part of the tender submission a complete, clause-by-clause response.

2. RESPONSE FORMAT

The tenderer shall respond to each clause with one of the following responses.

Should the tenderer wish to clarify or amplify the response, then the clarification or amplification shall not change the given meaning of the response statement.

Response	Meaning
Complies	The equipment/system offered complies fully in all respects with the specification clause.
Substantially complies	The equipment/system offered does not comply fully but offers most or a substantial part of the requirements of the particular clause. Compliance in excess of 75% of the requirement qualifies for this category. Areas of non-compliance must be clearly identified and explained.
Partially complies	The equipment/system offered provides only a part of the requirements of the clause. Less than 75% compliance with the clause should invoke this response. Areas of non-compliance must be clearly identified and explained.
Does not comply	The equipment/system offered does not provide the requirements of the particular clause.
Accepted	The tenderer understands and accepts the conditions imposed or enunciated by the particular clause and has included provision for such in the tender.
Not accepted	The tenderer does not accept the condition imposed by the particular clause and as such is not included in the tender. Reasons for non-acceptance must be given.

3. PRODUCT ACCEPTANCE

The successful tenderer will be required to demonstrate their competence to supply, install, commission, and maintain the products proposed in the tender submission as follows:

- Provide a letter of reference from the product manufacturers confirming the tenderer's status with the manufacturer, advising:
 - exclusive or non-exclusive agreement to provide the system in the geographical territory for this specific project,
 - the tenderer will be fully supported by the manufacturer in meeting the requirements of this specification.

The tenderer shall provide evidence of competency in carrying out the following areas of work:

- installation management,
- system configuration,
- system commissioning,
- system maintenance.

When working on the installation of the ISMS, each employee of the successful tenderer shall be required to carry an identification card issued by product manufacturers and/or government accredited bodies displaying evidence of current training, the type of products they may install, and indicating the level of training.

4. FUNCTIONAL OVERVIEW

The ISMS shall allow multi-site configuration and be able to be managed by one or more of the connected sites.

The ISMS shall include in the core product code (but not be limited to) the following:

- access control,
- alarm management,
- personnel management,
- CCTV integration,
- visitor management,
- guard tours,
- perimeter deterrent and detection.
- Time and attendance

-
- Fire detection systems
 - PA/EVAC systems
 - Generator and UPS/Invertor monitoring and control

The ISMS shall provide a means to control access through nominated doors having electric locking door status monitoring and token or biometric access control readers. Access rights associated with a presented access token or biometric identifier shall be checked for validity based on token or identifier, access area, access time and any other access management function defined in this specification. All validity criteria shall be stored at the IFC. Access shall be granted or denied dependent on the access privilege. Access privileges shall be programmed in a variety of ways to allow flexibility as defined elsewhere in this specification.

The ISMS shall provide access control in elevators enabling access to any combination of floors over specified time periods. The interface to the elevator manufacturers equipment shall be by either low level interface (relay outputs) or by a high level (data) interface.

The ISMS shall monitor the condition of inputs. The ISMS shall be able to be programmed to apply a variety of conditions to the way in which these inputs are monitored and shall enunciate the condition of such inputs in accordance with such programming.

The ISMS shall provide a fully functional intruder alarm system including entry and exit delays where intruder detection sensors are connected to system inputs. The intruder alarm ISMS component shall be fully integrated with the access control aspects of the system. It shall be possible to set (secure) or unset (unsecure) areas from any access control reader associated with an area, access control reader with keypad, AMT, or as required from defined central control locations.

The ISMS shall provide an integrated software facility for the design and production of photo ID cards.

Connection between ISMS servers and IFCs shall be achieved using cabling supporting the TCP/IP protocol. The network connection must be on-board the IFC. Interface transceiver units (Ethernet to RS485, RS232 etc) are not acceptable.

The ISMS shall have IPv6 address support for all TCP/IP network devices.

IFCs must support peer to peer communications for input and output communications between IFCs. Systems that require a server for communications between panels are unacceptable.

All data communication between the ISMS and IFCs shall use an industry standard asymmetric encryption algorithm for mutual authentication and session key negotiation. This algorithm shall be equivalent to ECC P-384 or stronger. Session keys shall be re-negotiated on a regular basis at intervals no longer than 30 hours.

All data communication between the ISMS and IFCs shall be encrypted using an industry standard symmetric encryption algorithm equivalent to AES-256 or stronger.

All data communication between IFCs shall use an industry standard asymmetric encryption algorithm for mutual authentication and session key negotiation. This algorithm shall

be equivalent to ECC P-384 or stronger. Session keys shall be re-negotiated on a regular basis at intervals no longer than 30 hours.

All data communication between IFCs shall be encrypted using an industry standard symmetric encryption algorithm equivalent to AES-256 or stronger.

All data communication between IFCs and intelligent edge devices such as readers and I/O devices shall use an industry standard asymmetric encryption algorithm for mutual authentication and session key negotiation. This algorithm shall be equivalent to ECC P-256 or stronger. Session keys shall be re-negotiated on a regular basis at intervals no longer than 30 hours.

All data communication between IFCs and intelligent edge devices such as readers and I/O modules shall be encrypted using an industry standard symmetric encryption algorithm equivalent to AES-128 or stronger.

All dry contact type input to field I/O modules must support four state monitoring with the ability to configure the resistance values of the state changes.

The ISMS shall report all events to the operator(s) as configured and shall produce and maintain a log of all system events, alarms, and operator actions.

The ISMS shall provide a means for an operator to extract information relative to the event log and system configuration and produce this information in the form of printed reports, emailed reports directly from the ISMS itself, screen displays, or exported files.

The ISMS shall provide for a GUI with site plans and interactive icons representing the location and real-time status of all monitored hardware within the ISMS.

The ISMS shall provide emergency evacuation reporting.

The ISMS shall be designed and manufactured by a company who shall be certified under the ISO 9001:2008 (or later) quality procedures.

Where applicable, equipment shall have the following approvals:

- FCC Part 15,
- CE approval BS EN 50130-4 Alarm Systems Electromagnetic Compatibility (Immunity),
- CE approval BS EN 55022 Emissions,
- UL294 Access Control,
- UL1076 Burglar Alarms,
- ULC-ORD-C1076.

Encoders and readers shall also meet:

CE ETS 300 683 Short Range Devices,

C-Tick AS/NZS 4251 Generic Emission Standard,

C-Tick RFS29.

The ISMS software shall be written in a fully structured, fully validated, and commercially available language that provides a strictly controlled development environment.

Comprehensive backup and archiving facilities shall be incorporated as an integral part of the ISMS.

The ISMS shall include partitioning suitable for multi-tenanted buildings. Users shall only be able to access those parts of the system which fall within their partition.

5. LICENSING

If system licensing is required, the license to use the system shall allow usage in perpetuity.

Details of the license model shall be provided in the tender response.

Licensing shall permit all operational requirements for a specific system. This shall include but not limited to:

- the live (operational) system,
- temporary test installations used for investigating configuration options or new software releases,
- secondary installations required for standby operation.

Updating of license content to make changes to the number of licensed items shall not require a server restart.

It is acceptable to require a restart to allow incorporating additional features to the license.

The license content shall be viewable from within the ISMS GUI.

6. SYSTEM REQUIREMENTS

The system shall be in commercial operation with the same or similar configuration as detailed in this specification and shall be available for inspection. A reference list of such similarly configured systems shall be submitted with the tender response.

The system described in this specification must have the following capacity as a minimum:

- Configured concurrent workstations 150
- Graphical site plans Unlimited
- Access readers Unlimited
- Elevators 1000 elevators of 256 levels each
- Fully supervised 6 state alarm inputs Unlimited

• Output relays	Unlimited
• Access control zones	Unlimited
• Schedules per day	100
• Schedule categories	50
• Holiday days	30
• Operators	Unlimited
• Concurrent operator sessions	100
• Cardholders	1,500,000
• Cardholder card issue levels	15
• Cardholder configurable data fields	>1000
• IFC	Unlimited

The system architecture shall be a tiered system consisting of:

- one installation of the head-end software application operating on a main server,
- operator workstations as a sub-set of the application installed on the server,
- IFCs managing the system in a distributed intelligence format,
- semi-intelligent sub-units (output modules, input modules, readers, etc) which rely on IFCs to function.

7. **SYSTEM SERVERS AND WORKSTATION INSTALLATION**

The server shall use a Microsoft Windows(64 bit) operating system. Server operating systems such as Linux, Unix, and OS X shall not be acceptable.

The operating system used by the system server shall be Microsoft Windows Server 2022.

The operating system used by the workstations shall be Microsoft Windows 10 Professional (64 bit) or Windows 11 Pro.

The database engine used by the system shall be one of the following:

- Microsoft SQL Server 2022, or
- Microsoft SQL Server 2022 Express.

Workstations shall support multi-monitor operation, allowing an operator to configure one or more monitors for each workstation.

Workstation display resolution shall be a minimum of 1920 x 1080 pixels.

Workstation shall be able to use up to 4Gb of RAM.

8. CENTRAL CONTROL AND SYTEM MANAGEMENT SOFTWARE

The ISMS servers shall use a Microsoft Windows operating system as defined previously.

The system database shall be a version of Microsoft SQL Server appropriate for the system size required. The version of Microsoft SQL Server is among those defined previously.

The connection between ISMS and Microsoft SQL Server shall use Windows Authentication.

The ISMS shall employ a server incorporating current generation design and components. The hardware specification, including processor speed, internal memory and hard disk size shall be specified by the supplier and must be sufficient to meet or exceed the capacity and throughput of the specified system.

The ISMS shall be capable of supporting configured concurrent Workstations. Workstations running terminal emulation software will not be accepted.

The ISMS shall automatically log and time/date-stamp all events within the system including intruder alarm set/unset events, access control events, operator actions and activity.

The configuration GUI shall make extensive use of menus and windows and require a minimum of operator training to operate the system proficiently. Systems requiring a script/program language approach to configure the system will not be accepted.

A free text notes/memo field shall be available for each logical/physical object to store abstract information relating to that item.

- The notes field shall support 128,000 characters of text.
- The notes field shall support word-wrap, insert, delete, cut, copy and paste functions.

The ISMS must be capable of receiving simultaneous alarm signals from remote locations without loss or excessive delay in their presentation to the operator. Any authorised operator should be allowed to acknowledge, view and/or process an alarm.

The ISMS shall be fitted with a real-time clock, the accuracy of which shall be preserved over the period of a mains power supply failure. Time synchronisation between the ISMS and Ethernet connected IFCs shall be automatic and not require operator intervention.

Operator selection of processing tasks shall be via menu selections. Authorised operators shall be able to process alarms, produce reports, and modify items without degrading system performance.

As a minimum the following operational and monitoring functions are required:

- program either a group or individual card readers with access control parameters, without affecting other card readers,
- program the access criteria for individual cardholders or groups of cardholders,

-
- store non access control data fields for each cardholder. The names of these data fields shall be user-definable,
 - authorise or de-authorise a cardholder in the system with the result reflected immediately throughout all access points in the system,
 - enable a card trace against selected cardholders so that an alarm is raised each time that cardholder presents their access card or token,
 - pre-program holidays so that different access criteria apply compared to normal scheduled days. The system must have a capacity to set at least 400 holiday days,
 - recognise and manage regional holiday requirements,
 - define as many access zones as there are card readers fitted,
 - allow or disallow individual cardholder access to any single, or group of card readers, in real-time,
 - log all ISMS and operator activity to hard disk as it is received at the ISMS server,
 - program alarm response instructions into the system so that these are presented to the operator when processing an alarm event,
 - enable an operator to enter messages against alarm events. This may be an enforced operator operation based on configuration on a per operator basis,
 - configure user-definable short messages to allow the operator to enter commonly used comments with minimal effort when entering messages related to alarms. For example, false alarm, user error, etc. These messages should also be assigned to keyboard shortcut keys to enable faster commenting on alarms,
 - temporarily override a cardholder, or group of cardholders, pre-programmed access criteria.
 - Update multiple AMTs display messages quickly using the bulk change feature

The operator GUI shall display a one-line plain language event message for every activity event (alarm or otherwise) occurring in the system. All activity logged shall be time and date stamped to the nearest second (hh:mm:ss). On having the appropriate operator authorisation, it shall be possible to drill down into the properties of each component that makes up that event. The event message shall advise:

- the time of event created at the IFC,
- the time the event was received at the ISMS server,
- the source of the event,
- any successful or unsuccessful access attempt,
- if the access attempt is unsuccessful, the reasons for the denial.

This includes but is not restricted to the following items:

-
- all card attempts,
 - all door alarms,
 - all operator activity including logon, logoff, and alarm response messages,
 - all alarm monitoring activations,
 - all communication link failures.

Time schedules for different days shall be configurable.

Regional holidays shall be configurable to allow for regional variations.

The system shall provide a detailed operator help file. This help file shall provide operators with text, audio, and video, help instructions and tutorials.

The system shall allow for searching of items configured within the system based on the following:

- item characteristics,
- related items,
- times related to events including within properties of a configured item (creation and modification events).

The system shall integrate with Microsoft Active Directory enabling cardholder and user records to be fully synchronised on a real-time, bi-directional basis.

- Integrations that use third party applications to synchronise between Microsoft Active Directory and the system shall not be acceptable.

The system shall allow for a separate biometric operator privilege.

The system shall be able to find unmigrated and duplicate DesFire cardholder keys.

ISMS shall be able to purge pending queued messages from IFCs as required by the user with this privilege.

ISMS shall be able to deploy IFC firmware as follows via an upgrade tool.

On demand.

On a predetermined schedule.

ISMS shall allow the user to track IFC firmware deployments status via the upgrade tool.

ISMS shall allow users additional options to manage ISMS functions via a web-based client safely and securely. Options shall provide an alternative to using the client-based application for the following:

- View Cardholder's History and activities.
- Manage cards (excluding printing and encoding) and credentials.
- Add cardholders and assign to Access Group.
- Remove cardholders.

The ISMS shall incorporate utilities that:

-
- Allow the health and security of the system to be checked with exportable reports.
 - Provide functionality to run pre-upgrade checks that identify any compatibility issues prior to a software upgrade.

ISMS shall allow bulk site configuration to:

- Enable importing and exporting as .csv files, all configuration items currently supported including system devices and Access Groups.
- These shall be able to be modified and re-imported to the existing system or used to import to a new system.

ISMS shall allow for configuration and setup of a read-only replica SQL database in a highly available environment in order to reduce the load on the primary SQL database.

ISMS shall support the redaction of the following Personal Identifiable Information in order to meet GDPR requirements:

- Cardholder Events
- Cardholder Information
- System software installation shall support command-line silent installation.

ISMS shall support cardholder case and accent sensitive searches.

9. COMMUNICATIONS AND DIAGNOSTICS

The ISMS shall automatically restart full and complete processing after a power failure.

The ISMS shall provide a full diagnostic log to enable system engineers to monitor system operations in the event of a system malfunction.

The diagnostic log shall be stored in a separate file on hard disk from all other data files.

The diagnostic log must be available without shutting down or pausing the ISMS.

The central control shall provide system diagnostic facilities which enable authorised operators or systems engineers to monitor and then tune the system performance (communications network performance tuning, for example).

ISMS shall be able to send the IFC its IP address

ISMS shall be able to accept requests from anywhere on the internet and connect these requests securely and easily to REST APIs hosted on an on-premise system using a web-socket tunnel between the ISMS and the API gateway.

API gateway shall have multiple redundant services internally allowing for zero-downtime upgrades, hardware and software fault tolerance and scalability.

API gateway shall use TLS client certificates for Rest API requests.

ISMS real-time data feeds shall integrate with Windows OS performance monitor

10. CYBERSECURITY

The ISMS manufacturer shall supply documentation detailing the cryptography used in the supplied products including:

- included digital certificates,
- database encryption,
- server to workstation connections,
- server to IFC connections,
- data at rest on IFC.

The ISMS manufacturer must provide proof of independent penetration testing for the release of software to be installed.

Vulnerabilities found in the ISMS software must be notified to customers via a CVE Entry for a minimum of two years after software release.

The ISMS manufacturer shall supply a software tool external to the ISMS server to test the installed server for vulnerabilities.

The system SMTP library shall support Microsoft office 365.

The system shall support a SQL Database monitor service which logs SQL Database login attempts.

Logins into the ISMS from the web-based client is secured with 2-factor authentication

The web-based client shall not store any sensitive data, data remains hosted on the customer's ISMS server.

11. MULTIPLE SERVER CONNECTIVITY

ISMS based on multiple servers shall be supported.

Each server shall communicate directly with its local IFCs.

Should a network failure occur between servers, each shall continue to communicate with their local IFCs.

Should a network failure occur between servers, operators shall be able to continue to manage the local system connected to their respective servers. This includes (but is not limited to) the following functions:

- manage alarms,
- override and manage doors,
- arm and disarm alarms,
- edit cardholders,

-
- run reports.

Alarms and events from all servers shall be able to be displayed on any or all of the system workstations.

The cardholder database shall be automatically replicated to all servers as a global entity.

Replication of cardholder changes shall occur as changes are made and not batch processed.

Communication between servers shall be peer to peer.

The multiple server environment shall allow for evacuation reports for each site on the multiple server system to be generated on one server, for one or more remote servers.

Operator GUI views and program access privileges shall follow the same rules across multiple servers as apply within a single server.

ISMS items configured on existing servers shall automatically be recognised by any servers added to the multiple server group. Likewise, ISMS items configured on the server(s) being added shall be automatically recognised by the existing multiple server group.

Use of software interface custom written modules or scripts to connect servers into a multiple server configuration shall not be permitted.

Manual or script re-entry of data for existing servers into any new servers being added to the multiple server group shall not be permitted.

Synchronisation of data across all servers shall be an automatic real-time function not requiring operator intervention or initialising.

Should communication be lost between two or more servers, the individual servers shall continue to function independently and shall resynchronise all changes made whilst off-line automatically after reconnection to peer servers.

Should a conflict occur resulting from two items being created in two or more servers whilst servers are off-line then an alarm shall be raised when the servers are re-joined advising of the conflict.

Should an existing record be modified in two or more servers whilst the servers are off-line then on reconnection, the modifications shall be carried out in time order of the modifications.

There must be a native tool within the operator GUI to remove redundant servers from a multiple server configuration. The use of scripts applications is not allowed.

12. GRAPHICAL OPERATOR INTERFACE

Configuration or operation using scripting or other forms of text-based programming will not be accepted.

There shall be a user configurable view, designed specifically for the task and the information needs of the operator.

Default operator views shall be provided covering the primary site management functions of:

- events,
- alarm management,
- cardholder management,
- access management,
- site monitoring,
- calendars and scheduling,
- macros,
- operator management,
- mobile device management,
- site wide system changes,
- reports.

The ISMS shall allow the creation of customised views to enable operators to access information relevant to a specific business workflow within one screen.

The operator GUI shall be fully configurable by an operator with authorisation to configure the GUI.

The operator GUI may be dynamically separated into multiple windows to allow for multi-monitor operation, closing the secondary GUI will automatically return navigation items to the primary GUI.

The primary operator GUI will always display an alarm count differentiated by alarm priority.

Each view shall consist of a navigation menu area and a dynamic viewing area as detailed below.

The navigation area shall provide a list of relevant data related to a specific workflow as defined by the task at hand.

It shall be possible to select and order the columns of data in the navigation area associated with alarm and cardholder views.

Dynamically updated search results shall be provided when typing into the search field for a cardholder view.

Selection of a line item in the navigation area shall cause the associated dynamic information viewing area to be populated with data relevant to the selected item.

Within the dynamic viewing area one or more data tiles shall be provided to display detailed data associated with the navigation area item selected.

Data tiles shall be able to be created based on a range of default tiles provided for this purpose.

Each data tile shall be configurable with the required data fields as determined by the function of the tile.

Data tiles shall be maximised to enlarge the display area for that data by single click operation. Another single click operation on this tile will return all tiles to original size and location.

When a data tile has been maximised, other tiles shall remain visible in thumbnail format, allowing a single click to make them the selected maximised data tile.

Where applicable, minimised tile icons shall display dynamic content.

There shall be provision for displaying data tiles within the dynamic viewing area that link to external sources.

The linked data tile shall allow either a URL address, PDF, or TXT file to be selected.

Navigation from a URL shall be configured either as:

- navigation enabled,
- restricted navigation allowing navigation to hyperlinks on the site but not to enter a URL,
- navigation disabled.

Auto refresh of a URL shall be configurable down to 1-minute resolution.

An event view shall be available with the following capabilities:

- allow the operator to view events in real-time,
- the displayed data columns shall be configurable,
- the columns shall be sortable,
- auto scroll capability.

The event view shall also allow the operator to search for and select historic events, even when they have been cleared from the real-time view window. This shall include:

- search based on time/date,
- search based on the source of the event,
- the selected historic event shall appear in the event window with the same relevant data as if it were a real-time event,
- display a count of the number of events which were found.

When a single event has been selected the following information shall be possible to be displayed:

-
- instructions for the operator,
 - details of the event,
 - site plan,
 - cardholder image (where appropriate to the event),
 - video camera feed (where appropriate to the event),
 - recent event history for the door (where appropriate to the event),
 - recent event history for the cardholder (where appropriate to the event).

The system shall support Microsoft Edge as the default browser if Webview 2 Runtime is installed on workstations.

Calls from supported intercoms shall be managed from a central location from within the GUI using a unified intercom viewer.

13. SYTEM OPERATOR MANAGEMENT

Operator establishment and maintenance shall be a restricted privilege.

It shall be possible to define specific ISMS privileges for a group of operators and an individual operator can be added or removed to this group without changing any other properties of that group or the operator than this relationship.

Operators (non-Admin) inactive for a specified time period can be configured to have the user account disabled.

Operator access to the operator GUI is to be restricted by means of a unique operator identifier and password.

It shall be possible to apply password restrictions that consist of (but are not limited to) the following:

- minimum password length,
- mixed case,
- mixed alpha and numeric characters,
- mandatory change of password after a defined period,
- remembering and rejecting at least 999 previously used passwords.

There shall be default password restrictions that cannot be disabled as follows:

- Passwords must not contain the login name, first name, or last name of the operator
- There shall be a file containing common passwords that will not be allowed, this file will be editable by the customer to strengthen or relax the disallowed passwords.

The system shall support an Active Directory Single Sign-On feature to allow access to the operator GUI without password if they are already logged into an authenticated Windows session.

Each operator shall have the authority to alter their own password.

Automatic logoff may occur after a preset time of up to 1440 minutes of operator inactivity.

It shall be possible to configure the system to only allow one simultaneous logon per operator.

It must be possible to allow or deny operators access to various menu functions.

It shall be possible to blend the right to view groups of system objects for different operators; i.e. an operator in building 1 can see alarms for building 2 but is not able to perform any function on them. An operator in building 2 has the inverse relationship and can only action alarms for building 2 but still view alarms in building 1.

Any menu option not available to an operator should be either greyed out or not visible.

It shall be possible for a suitably authorised operator to view all connected data sessions on the ISMS, and the following minimum information shall be displayed:

- device name,
- login credential,
- session type, i.e. operator GUI, mobile application, data connection OPC/XML etc,
- session status,
- it shall be possible for a suitably authorised operator to terminate any data session.

14. CARDHOLDER MANAGEMENT

The cardholder database shall be structured so that the name field is the master field for each record. A background unique identifier may be used as the key field for each record, but this must not be required by an operator to identify a cardholder. Use of the card number as the key field is not acceptable.

The system must allow at least 15 issue levels per card or token. This must deny access and raise an alarm to the operator when a wrong issue level is presented to a reader.

Cardholders must be able to be issued with more than one unique access token (i.e. access card, biometric identification, and vehicle token) whilst maintaining only one cardholder record in the database.

Where a PIN is assigned to a card three consecutive or repeating digits shall not be allowed.

Where biometric identification is required, the biometric data shall be a property of the cardholder record.

Encoding and printing cards shall be properties of the cardholder record.

The options for encoding and printing shall be:

- print card,
- encode card,
- print and encode card in a single operation.

It shall be possible to prevent the duplication and/or re-printing of cards on a per operator basis.

Where a PIN is assigned to a card it should be stored in the database of the ISMS not as part of card data.

There must be an option to save a copy of the PIN for later retrieval for forgotten PINs, if this option is not selected then a cardholder's PIN will be saved in a one-way hash to the database.

Card numbers shall be enrolled against a cardholder by manually entering the card number or in the case of any Mifare technologies, a reading device connected directly to a workstation.

Access groups shall be linked to cardholders by both assigning access groups to cardholders or cardholders to access groups.

At least 64 user-definable data fields shall be provided which may be selectively reported on.

Cardholder data fields shall be able to be configured as:

- text; user data may be entered,
- text list; operator selects text from a pre-prepared list of text strings,
- numeric; operator must enter numeric data,
- date; calendar dates may be entered based on the workstation date format,
- default value; the field has a default value assigned,
- no default value; default value disabled,
- image; the field may only contain an image,
- email/mobile; the field contains an email address or mobile number to be used for communication by the ISMS,
- required field; the value may not be null,
- unique values; data must be unique from all other cardholder records.

Cardholder data fields shall support regular expression rules to ensure data accuracy. Examples: @ in email addresses; employee codes are in the correct format.

It shall be possible to group or filter cardholders for the purposes of editing access, generating reports, and assigning operator privileges.

The following information fields shall optionally be displayed on the cardholder editing window:

- the date when a cardholder record was created,
- the date when the record was last modified,
- access groups that a cardholder is a member of,
- for ease of programming, cardholders shall be grouped into access groups sharing the same access criteria and default cardholder data fields,
- it shall be possible to allocate start and end dates and times for an access groups membership,
- cardholder additional data fields,
- images which may include photos, signatures etc,
- allocated cards,
- it shall be possible to enter an expiry date/time for the card,
- cardholder qualification information relating to fields such as “Security Clearance”, “Safety Induction” etc,
- a URL link to additional information which may be located on the customer intranet, or the internet.

Access shall have start and end dates and time to within one minute.

The system shall be capable of importing database information, on selected cardholders, from other systems and be capable of exporting that cardholder’s data, either with or without controlled alteration or amendment to other databases.

The system shall support the capability to allow bulk changes to cardholder records. It shall be possible to carry out the following changes as a bulk change:

- delete selected cardholder records,
- change custom cardholder data fields
- change cardholder card details,
- change cardholder access options.

The system shall support the ability to bulk change the system division that database objects are assigned to.

A bulk change shall be able to be saved and scheduled to run at a later time.

A window shall be provided to show details of created, saved, edited, pending, successful, and failed bulk changes.

A personal user code (4 to 8 digits) shall be a property of the cardholder record to allow access via readers with a keypad and to arm and disarm alarms.

Operator management shall be a property of the cardholder record.

A change history record associated with each cardholder record shall list all changes made to a cardholder record, including details of which operator or API login made the changes.

The system shall support an event trail for the cardholder which details recent card usage events for the cardholder as well as operator events which have modified the cardholder record.

The number of prior events to be shown or prior length of time to be covered shall be configurable.

The system shall allow different prior length of time / number of prior events to be displayed for different operators.

The cardholder record screen shall display a real-time event trail of cardholder activity.

The system shall allow an operator to search for a cardholder by entering any part of their first and/or last name, in any order and separated by a space if using both. After three characters have been entered the system shall automatically return matching results and filter these dynamically as the operator continues to type.

The system shall allow the cardholder search fields and search results to be configurable. The system shall allow different operators to use and see different search fields and search results for cardholder administration tasks.

The system shall allow the information returned for a cardholder and visible to the operator to be configurable and include any sub-section of the total information stored in the cardholder record (e.g. custom data fields, cards, access groups, biometric information etc). Different operators shall be able to view different sub-sections of the cardholder information.

It shall be possible to locate a cardholder record by presenting their card to a reading device connected directly to an operator's workstation.

The system shall allow cardholder information to be viewed and updated in one screen.

Configuring operators shall, subject to the required privileges, be able to design a single screen cardholder management view adapted for the specific screen resolution of the operator(s) who will use the view, to ensure best use of available screen real-estate.

The system shall be able to display up to 30 historical cardholder activity items instantly in a viewer.

15. PHOTO BAGGING AND IMAGE MANAGEMENT

The ISMS must have an integrated card design program. Systems offering a separate card design program where card designs must be created in alternate drawing programs and imported are not acceptable.

The ISMS shall provide a means to:

- electronically capture images,

-
- store the images in the server database,
 - integrate those images into a pre-designed ID card from within the system,
 - produce an integrated and finished identification card.

The ISMS must be capable of storing at least three images per cardholder.

The ISMS offered shall capture images in 24-bit colour and at least 800 x 600 pixel resolution, using standard video capture hardware offering a TWAIN, Direct Draw standard interface, or a USB digital camera.

Images must be able to be cropped after capture to optimise the image size within the desirable image area. This size of the movable cropping box must be user-definable.

The image capture editing controls must be integrated into the system software.

The ISMS shall store images in the JPEG compression format. User definable compression rates shall be easily selectable by the operator, a minimum of three levels of JPEG compression are required.

The facility to import background images from other sources into the card designer must be available.

The ISMS offered shall be capable of importing image files, for use in either card layout or cardholder images, from at least the following formats:

- JPEG,
- Windows BMP,

The card design must be capable of incorporating, storing, printing and displaying bar-code information and must support the following bar-code formats:

- EAN 13,
- EAN 128,
- UPC A,
- UPC E,
- Code 39,
- Code 128,
- Interleaved 2 of 5,
- Codabar,
- Telepen,
- PDF417.

The card design must be capable of user-selecting up to 16.7 million colours with a custom colour palette available.

Card design must be accomplished using drag and drop options via a mouse.

Card design must support both sides of the card.

The system shall be capable of linking data relating to the cardholder and printing it the card. This data shall include (but not be limited to):

- first name,
- last name,
- card number (displayed as text and/or barcode),
- card issue level,
- expiry date,
- personal data as defined in the cardholder database.

The system must be capable of using all installed word processing fonts and must also be capable of normal text manipulation including, text sizing, left and right justification, centring, bolding, underlining and italicising.

The image files that are selected to incorporate into the card design must be scalable on the card. When scaling the image, the card designer must offer automatic aspect ratio adjustment throughout the size range.

The system shall be capable of producing hard copy output of images and data using any standard MS-Windows printer.

Cards must be capable of either landscape or portrait printing and barcodes must be capable of either vertical or horizontal orientation on the card when printed.

16. INTRUDER ALARM SYSTEM

The ISMS will incorporate a fully functional intruder alarm system.

All inputs globally within the system must be able to be utilised as intrusion alarm inputs to allow intruder detection sensors to be connected to the system.

All outputs anywhere within the system shall be available for intruder alarm purposes such as sounding remote sirens etc.

Arming and disarming the intrusion detection system shall be either by using card readers, alarm management terminals, key-switches or schedules.

It shall be possible for the system to cause readers to beep during entry and exit delays.

It shall be possible for the system to active outputs during entry and exit delays.

It shall be possible to configure the system to isolate faulty external devices so as not to trigger false alarms.

It shall be possible to configure the system to fail to arm if an input point is active.

It shall be possible to configure the system to fail to arm if an input point has unacknowledged alarms.

It shall be possible for the system to cause readers to beep when alarms are present in the system.

It shall be possible to set the system to a test mode to allow for testing and maintenance.

The intruder alarm zone and the access zone for an area shall be treated as separate logical items.

The intruder alarm system shall provide a dependency feature whereby an alarm zone does not go into the set state until all dependent alarm zones are in the set state.

- If the alarm zone is set (armed) and the access door is secure:
 - A cardholder shall require authorisation to both unset (disarm) the intruder alarm zone, and to access the access zone to be allowed access.
 - If the cardholder is not authorised to unset the alarm zone or not allowed to access the access zone, then access shall be denied.
- If the alarm zone is unset (disarmed) and the access door is secure:
 - A cardholder shall require access to the access zone only for access to be allowed.
 - If the cardholder is not authorised to access the access zone, then access shall be denied.
- For normal operation, after an authorised token is presented, and access is granted, then the alarm zone shall remain unset after the door relocks.
- As an optional function, the alarm zone may auto-set after a predetermined time period.

When specified, alarm monitoring may use a connection with central alarm monitoring stations via digital communicators using Contact ID format, connected directly to the IFC panels.

Connection with central alarm monitoring stations may be by TCP/IP or cellular networks.

- It shall be possible for alarms from one IFC to be transmitted via a second IFC where the digital communicator is installed. (Peer-to-peer communications).
- Digital communicators are to be able to communicate alarms from all system IFCs, independent of system server.
- The system shall report and log all digital communicator activity and the reason for any failure to communicate.
- The system shall provide for up to two back up communicators on different IFCs to provide automatic backup capability should the designated digital communicator fail to operate on the appropriate alarm condition.

Cardholders shall be assigned to groups, to which any combination of the following intruder alarm privileges relating to the operation of the system may be assigned:

- unset intruder alarm zones,
- set intruder alarms zones,
- status of alarms and inputs on AMT,
- acknowledge alarms,
- shunt inputs,
- force-arm alarm zones,
- auto-isolate alarm zones.

17. ALARM MANAGEMENT

The ISMS shall provide entry and exit delays for the setting (arming) and unsetting (disarming) of alarms.

The entry delay shall be configurable from 0 to 999 seconds in increments of one second.

An optional audible warning must sound during the entry delay (from the time the alarm occurs to the time that the zone state is changed). It must be possible to designate specific card readers and Alarm Management Terminals (AMTs) to sound entry delay warning beeps. Selected output relays should also be able to be operated during the entry delay period allowing suitable sounders to be connected at required locations.

The exit delay shall be configurable from 0 to 999 seconds in increments of one second.

An optional audible warning must sound during the exit delay (from the time that the alarm occurs to the time that the zone state is changed). It must be possible to designate specific card readers and AMTs to sound exit delay-warning beeps. Selected output relays should also be able to be operated during the exit delay period allowing suitable sounders to be connected at required locations. This applies to both manually and automatically changing the state of a zone in the case of automatically changing the state of a zone the exit delay and audible warning gives people working late in the building time to unset the alarms or leave the building.

The system shall include an alarm escalation as a feature. The new event shall correspond to the original alarm but will have a higher priority and may include a different set of alarm relays to operate.

Escalated alarms shall be able to be displayed in a window specifically provided for this purpose.

Alarms shall be able to be escalated under the following conditions:

- Escalate if the alarm is not acknowledged for a period of time. This must be configurable from 0 to 9999 seconds in increments of one second.

-
- Escalate if the alarm point remains in an active state for a period of time. This must be configurable from 0 to 9999 seconds in increments of one second.
 - Escalate if a user defined zone contains a specified number of unacknowledged alarms from any number of alarm points. This must be configurable from 0 to 99.
 - Escalate if there are two events from the same alarm point within a user-defined period of time. This must be configurable from 0 to 9999 seconds in increments of one second.
 - Escalate if there are two events from different alarm points in a defined group within a user-defined period of time. This must be configurable from 0 to 9999 seconds in increments of one second.

An additional option of advanced Alarm management will allow:

- Escalation to supervisors when alarms are not processed within a set timeframe.
- Operators to manually escalate alarms to a higher level operator.
- Operators to start and stop receiving alarms whereby alarms are automatically re-distributed to other active operators.

It shall be possible to have automatic time-based setting and unsetting of alarms.

It shall be possible to configure the system such that events (such as a card badge or operation of a key switch connected to an input) can change the state of an alarm zone.

Authorised cardholders shall be allowed to set and unset alarm zones by:

- code access at an AMT,
- operation of the card plus PIN reader at an AMT,
- presenting a valid access card to a card reader associated with the alarm zone, twice within a nominated time period (double card badging).

It shall be possible to set and unset multiple alarm zones from an AMT.

All alarm occurrences shall be presented at the ISMS within 5 seconds of their occurrence at the remote field device.

All alarm events shall be viewable from an alarm stack.

It shall be possible to view all alarm events by clicking on interactive site plan icons that, because of their changing audible and visual states, indicate the presence of alarms.

All alarm events arriving at the central control shall be time-stamped with the time they occurred and the time they were logged at the ISMS.

All alarm events shall have a user-definable alarm priority assigned. A minimum of 8 alarm priority levels plus non-alarm event and ignore event shall be provided.

Incoming alarms shall be presented in the alarm stack according to their assigned priority with the highest level at the top. Alarms with the same priority shall be presented in time order.

It shall be possible to assign a different audio warning sound to each alarm priority.

It shall be possible to assign a system definable colour to each alarm priority.

Identical consecutive alarms that occur within a predefined time span shall be report as a single alarm with the number of occurrences reporting as a flood alarm quantity.

The ISMS must be able to control the priority assigned to any alarm activation according to a schedule. This means an alarm activation may be programmed as “Low Priority” during office hours and “High Priority” at other times.

It shall be possible to nominate an input (e.g. smoke, fire, or gas detection) as an “Evacuation Input” in which case certain doors within the site will change immediately to free access.

The ISMS shall support two-stage alarm processing as:

- Acknowledge alarm:
 - An acknowledged alarm shall remain in the alarm stack and be easily identified as having been acknowledged but not yet processed.
 - The ISMS shall record in the hard disk activity log that the operator has acknowledged the alarm.
 - A second alarm from the same source as the acknowledged alarm shall be indicated as a new alarm.
- Process alarm:
 - A processed alarm shall clear from the alarm stack.
 - The ISMS shall record in the hard disk activity log that the operator has processed the alarm.

The system shall allow an operator to multi-select contiguous or non-contiguous alarms in the list to add a note, acknowledge, or process all selected alarms in one action.

The alarm list shall support mandatory fields of alarm time, alarm priority and alarm state.

the ISMS shall allow a suitably privileged operator to configure any of the following additional fields to be visible in the alarm list and to configure their order:

- full alarm message,
- related cardholder name,
- acknowledging operator name,
- alarm Zone,
- alarm source,

-
- related access zone,
 - event type,
 - event group,
 - division of the alarm source,
 - count (occurrences of alarm).

It must be possible for an operator to sort the alarm list by any of the available fields.

The ISMS shall display a summary of alarms, by priority, which is always visible to the monitoring operator and updated dynamically as new alarms occur or existing alarms are actioned.

The alarm summary shall indicate if there are any unacknowledged alarms for a given priority.

The ISMS shall allow configuration of filtered alarm lists. Alarm lists shall be filterable based on any combination of selected divisions, escalation status or alarm priority.

The ISMS shall allow different information to be configured and displayed to a monitoring operator based on the type of alarm.

“Door Open Too Long” alarms must display selected and configurable information. Including, as an example, the photo and contact details for the cardholder who left the door open, i.e. last successful access.

Cardholder related alarms shall automatically display recent events and selected information (name, photo, personal details etc.) for the cardholder causing the alarm.

An active alarm shall not be able to be finally processed and cleared from the alarm window until the cause of the alarm has been removed and the alarm condition has returned to the normal state.

Pre-programmed alarm instructions shall be available for the operator to provide instructions for acknowledging and processing each alarm.

- Alarm instructions shall have the following features:
 - Default alarm instructions shall be able to be programmed and automatically applied to all events of a common type e.g. all wrong PIN events applicable to all readers.
 - Individual alarm instructions shall be able to be programmed and applied to individual alarm events.
 - A repository of configurable data fields of volatile information shall be available when programming alarm instructions, and applied to alarm instructions via text tags or drag and drop.
 - When the data fields in the repository are updated, the linked alarm instructions shall automatically update with the current value when displayed to an operator.

-
- The alarm instruction text shall be able to be formatted using common text formatting features including but not limited to:
 - bold, italic, underline,
 - text colours,
 - left, centre, and right justified,
 - bulleted text,
 - standard Microsoft Windows font types and sizes.
 - It shall be possible to copy and paste alarm instructions between alarm events.

The alarm window shall allow the operator to enter a comment. Such comment will be date/time stamped by the ISMS and recorded against that alarm event in the audit trail.

- When required, a pre-defined list of alarm responses shall be available for operators to select the appropriate response to an alarm. The alarm responses shall be user configurable to suit site requirements.

Keyboard function keys (F1 to F8) shall be mapped to the first 8 alarm response messages to insert the associated message via keyboard as required.

ISMS shall allow the user with the appropriate privilege to mute alarms in the alarm stack.

18. CLASS 5 ALARM SYSTEM

The system shall be capable of being installed and configured up to Class 5 level of the AS/NZS 2201 Intruder Alarm System standard.

The Class 5 system shall include provision of Class 5 compliant end-of-line modules for alarm sensor communications protection.

The Class 5 system shall include provision of Class 5 compliant cabinetry, including Class 5 compliant locking mechanism, tamper sensor, and vibration sensor.

The Class 5 system shall include provision of Class 5 compliant power supplies, capable of:

- recharging up to 100Ah of battery backup,
- recharging all batteries within 48 hours of power being restored.

The Class 5 system shall include support for a battery backup system which meets the following:

- a minimum of 16 hours of battery backup for a monitored system,
- a minimum 24 hours of battery backup for a non-monitored system.

The Class 5 system shall include provision of Class 5 compliant AMT, supporting the following:

-
- user authentication with card + 6-digit minimum PIN length,
 - alarm arming,
 - alarm disarming,
 - manual alarm condition isolation,
 - automatic alarm condition isolation.

The Class 5 system shall include provision of Class 5 compliant controllers, supporting the following:

- data communications authenticated utilizing a minimum of ECC P-256 to the following;
 - AMT
 - end-of-line modules
- data communications protected utilizing a minimum of AES-128 to the following;
 - AMT
 - end-of-line modules
 - dedicated hardware cryptographic key storage, compliant to the FIPS 140-2 specification.

19. ACCESS CONTROL

The ISMS shall provide complete flexibility and be capable of programming an unlimited combination of access control, security alarm, and I/O parameters subject only to performance and memory limitations within each IFC.

For ease of programming cardholders shall be grouped into groups sharing the same access criteria.

Individual cardholders may be assigned with an extended door unlock time, as may be required by cardholders with a disability.

It shall be possible to assign an individual cardholder to an access group on a temporary basis with predetermined start and finish times.

- During the period of temporary access, the cardholder shall have the rights of the group to which they have been assigned in addition to any permanent access rights they may have been assigned.
- The access group details page shall display both permanent and temporary access members with the status of temporary members shown as:
 - pending (with the start and finish times),
 - active,

-
- expired.

Any cardholder or access group in the ISMS shall be able to be programmed to have access to any combination of controlled doors in the ISMS with each period of access for each door controlled to within the nearest minute.

The IFC shall check entry based on all of the following criteria:

- correct site code,
- authorised card in database,
- correct issue number,
- authorised door / access zone,
- authorised time of day,
- valid card holder analytics,
- correct PIN (If PIN entry is required),
- double entry (anti-passback, anti-tailgating, or escort modes).

Anti-passback mode shall be able to be configured in any of the following modes:

- disallow second access to an area if a valid exit has not previously been registered and generate an alarm (hard anti-passback),
- allow second access to an area if a valid exit has not previously been registered but generate an alarm (soft anti-passback),
- exclude specific access groups from the rules defined in (a) and (b) above.

Anti-passback rules shall be able to be reset by:

- automatically after a preset period after valid entry,
- automatically at a standard time each day,
- automatically on exit from site,
- manually as an override.

The ISMS must support global anti-passback allowing multiple access zones to be linked for anti-passback, across multiple IFCs utilising encrypted peer-to-peer communications.

The IFCs shall not rely on the server for anti-passback operation. Global anti-passback shall work across multiple IFCs, even if the server is offline.

The anti-passback capability of the ISMS shall enforce anti-passback on a single cardholder for the use of multiple credential types (e.g. mobile phone, keyfob, Mifare card).

Anti-tailgate mode shall be able to be configured in any of the following modes:

-
- disallow exit from an area if a valid access has not previously been registered and generate an alarm (hard anti-tailgate),
 - allow exit from an area if a valid access has not previously been registered but generate an alarm (soft anti-tailgate),
 - exclude specific access groups from the anti-tailgate rules.

Anti-tailgate rules shall be able to be reset by either:

- Automatically after a preset period after valid entry.
- Automatically at a standard time each day.
- Manually as an over-ride.

The IFCs shall not rely on the server for anti-tailgate operation. Global anti-tailgate shall work across multiple IFCs, even if the server is offline.

The anti-tailgate capability of the ISMS shall enforce anti-tailgate on a single cardholder for the use of multiple credential types (e.g. mobile phone, keyfob, Mifare card).

Every incorrect PIN attempt shall be notified at the central control as an alarm condition.

Each reader shall be capable of automatically switching the access mode of a door at different times of the day based on control parameters received from the ISMS. The following access criteria modes are required:

- free access (no credential required),
- secure access (credential required),
- secure and PIN access (credential and PIN required),
- specific users exempt from requiring secure and PIN for accessibility purposes,
- override from reader - members of certain access groups shall be able to change the access and PINs mode of the door at certain times,
- dual authorisation - access is granted when two different but legitimate cards are presented within a given time frame,
- escort - a second card is required to be presented from a cardholder who is nominated in a specified access group,
- shared code - The ISMS operator determines what the code will be and programs this into the ISMS. Access is allowed through the door when the correct 4-digit code is entered.

Cardholder access reporting to the ISMS and logging in the audit trail shall be configurable in two modes:

- only when there has been a successful presentation of a valid access card or token and the door open sensor has detected the door has opened,

-
- whenever there has been a successful presentation of a valid access card irrespective of whether the door has been opened.

Readers with integrated PIN pads, or biometric readers using identification shall provide an “Entry under Duress” facility.

- Duress shall be initiated by the cardholder either by incrementing the last digit of their PIN number by one. Duress on biometric readers shall be initiated by the cardholder presenting their pre-enrolled “Duress finger”.
- There must be no indication of a duress entry at the reader.
- When a duress alarm is raised at a reader a critical priority “Duress Alarm” shall be displayed at the ISMS.
- It must be possible to configure the ISMS such that duress or other selected critical alarms pop to the front of the display, ensuring immediate operator attention. The existence of lower priority incoming alarms shall be visible to the operator but must not interrupt their current task.

Zone counting shall be available to provide real-time counting of cardholders in access zones.

- The zone count shall be viewable on the Site Plan Access Zone object.
- The result of the number of cardholders in the zone being outside of the specified range(s) shall generate an event or an alarm, depending on ISMS configuration.
- The minimum and maximum numbers of cardholders in a zone before an event is generated shall be configurable.
- It shall be possible to set a “grace time” (in seconds) to allow the zone count to be outside the minimum within the mid-range or outside the maximum number of cardholders, without generating an event.
- It shall be possible to assign a specific message for each of the minimum, mid-range, or above maximum conditions.
- It shall be possible to set up the ISMS to prohibit one cardholder being alone in a zone by:
 - requiring two valid but different cards to access a zone should the zone count reports zero cardholders in the zone,
 - requiring one card to access a zone should the zone count report two or more cards in the zone,
 - requiring one card to exit from a zone should the zone count report three or more cards in the zone,
 - requiring two valid but different cards to exit from a zone should the zone count report two people present,

-
- prohibiting exit from a zone and generate an alarm if the zone count reports one cardholder present.
 - It shall be possible to increment and decrement zone counting based on physical inputs not related to access events.
 - It shall be possible to increment and decrement zone counting based on logical inputs not related to access events.
 - It shall be possible to schedule an access zone for a “First Card Unlock” mode, whereby the access zone is scheduled to go to free access, but only when a suitably privileged card is badged at the reader. All other cards will be granted access, but will not be able to set the door to free access unless they have the “First Card Unlock” privilege.
 - It shall be possible for suitably privileged cardholders to toggle the access mode of a reader between free and secure by badging their card at the reader twice in quick succession.
 - It shall be possible for suitably privileged cardholders to log on to a reader with a keypad either by a credential or credential and PIN and change the access mode of the reader to either free or secure.
 - In addition to unlocking a door when granting access, it shall be possible to activate an additional output or macro which is uniquely related to the cardholder or access group to which they belong.
 - It shall be possible to “lock down” specific areas of a site such that cardholders who would usually have access, are denied access. cardholders with suitable privileges such as security personnel will still have access. The “lock down” should be activated and/or cancelled by the following methods:
 - clicking an icon on a site plan,
 - triggered based upon an event within the ISMS,
 - triggered from an input.

20. PERSONNEL IDENTIFICATION VERIFICATION

The ISMS shall be certified as complying with the requirements of FIPS 201-2 on the GSA FIPS 201-2 Approved Products List (APL)

The ISMS must provide a fully integrated solution that will harvest the information from the PIV card, validate it with the online certification authorities and store that information on the server database, this must include as a minimum:

- the PIV certificate,
- the CAK certificate,
- the biometric template,
- the cards “printed Information”,

-
- the full FASC-N for a PIV card or the GUID for the PIV-I card.

The ISMS shall provide an interface to allow integration to Enterprise Identity Management systems. This interface shall allow certificates and images to be imported into the ISMS database.

At all times the ISMS shall use the full FASC-N or GUID as the credential number in the ISMS and it shall not be allowable to use a truncated or non-unique representation for access control.

All access validation shall be done at the IFC. This shall include:

- CAK signature check,
- CAK expiry or notBefore Check,
- CAK and PIV certificate revocation – based on cached data,
- The challenge of the PIV card's CAK private key.

The ISMS must implement the CAK Authentication single factor access mode authentication.

Contactless CAK Access decisions, card presented to door released, shall take no longer than the following times:

- RSA 2048-bit keyed CAK Certificate: 3 Seconds,
- ECC P256 bit keyed CAK Certificate: 1.5 Seconds.

The ISMS must validate all PIV credentials via the external Certification Authorities at configurable periods between 1 hour and 24 hours.

Card readers must communicate to IFCs via a bi-directional supervised protocol on a physical RS485 transport layer. Additionally, the protocol shall be encrypted using AES-128 keys and authenticated using 256-bit Elliptic Curve Cryptography.

Each card reader shall have a manufacturer's unique serial number and the ISMS must prevent unauthorised reader substitution.

Card readers and IFCs must be able to show compliance to FIPS140-2 level 1 for communications and validation cryptography and FIPS140-2 level 3 for key storage.

ISMS shall support on demand PIV certificate validation

21. SITE PLANS

It shall be possible to manage and monitor alarms, overrides, the general real-time status of site items and open doors through the operator GUI with the use of interactive dynamic site plans, icons.

The designing and editing of a site plan shall allow:

- The basic editing tools to assist in the design and creation of the site plan.
- Assigning icons to ISMS functions and place these at any position on a site plan.
- Provision for drawing lines and shapes to form objects shall be available. These objects shall be able to be associated with ISMS items allowing ISMS item status to be visually indicated by the object.
- It shall be possible to place free text onto a site plan.
- An optional grid shall be available with snap-to-grid available for all objects and vertices.
- Individual objects within a site plan shall be able to be moved behind and in front of other objects using a layer scheme.
- An alignment tool shall be provided to align groups of objects in both x and y dimensions.
- External drawings shall be able to be imported into the ISMS from external drawing software. The ability to import common and the following drawing formats shall be supported:
 - EMF,
 - PDF,
 - PNG,
 - WMF.
- It shall be possible to design and load icons from external software for use in the ISMS.
- It shall be possible to design interactive buttons to reside on site plans. On activation, the buttons must be capable of performing multiple overrides for ISMS items simultaneously.

When an object is selected on a site plan, it shall present an interactive menu to the operator. All the following functionality must be included:

- View the current status of a door, input, or output,
- override a door, input, or output,
- monitor and acknowledge an alarm,
- open an access-controlled door,
- Change an unlock schedule on a door,
- move from one site plan to another,
- activate an intercom,

-
- override an alarm, access, or perimeter fence zone state,
 - generate a report.

Site plan usage shall support touch-screen technology and preclude the use of a mouse right-click as a separate function.

Site plans shall be capable of pan and zoom functionality.

All open site plans shall be updated immediately if that site plan is amended at any workstation.

Icon names shall use the item name by default, but a shortened name shall be configurable so as not to clutter the site plan with text.

The ISMS shall support a search functionality that when searching for an object, it will return a site plan containing the object.

There shall be provision for sending a copy of the currently visible site plan to a printer, email, or Windows clipboard, natively within the ISMS workstation application.

The site plan shall provide a means to show or hide objects at predetermined zoom levels to assist in reducing clutter on a highly populated plan.

When zooming out of the site plan, objects must amalgamate into a summarised indicator.

A site plan must support multiple floor layers in a single site plan item.

Whilst panning around a site plan, a secondary site plan must automatically present itself when the display pans over the location of that site plan that represents that sub-area.

Site plans shall allow icons for third party doors

Site plans shall allow background colour selection

Site Plans shall allow the user to customise its orientation

Site plans shall allow the user to implement the following:

- Provide options to hide and display items dependent on zoom levels
- Embedded site plans
- Have the ability to link separate panels and incorporate related items

Site plans shall allow intercom integration allowing for the following functions

- A fold away intercom Call queue which drives the navigation to the relevant intercom on the site plan
- Ringing behaviour on the intercom/door icons
- Popup controls to allow management of an intercom call

22. GUARD TOURS

The ISMS shall support multiple guard tours between check points.

- There shall be no imposed limit on the number of guard tours that can be configured.

Check points shall be card readers, inputs, or outputs.

- There shall be no imposed limit on the number of check points.

Multiple guard tours must be able to run concurrently.

The guard tour shall allow for flexible and configurable timing between check points which shall have (but not be limited to) the following:

- transition time;
 - the time period that it should take the guard to move from the last check point to the next check point,
 - this shall be configurable in hours, minutes and seconds,
 - the time shall be uniquely configurable for each check point,
- deviation;
 - the time allowed for the guard to be early or late at the check point,
 - this shall be configurable in hours, minutes and seconds,
 - the time shall be uniquely configurable for each check point,
- late;
 - the time period that has elapsed since the guard was expected at the check point wherein they are now considered as late to the check point,
 - this shall be configurable in hours, minutes and seconds,
 - the time shall be uniquely configurable for each check point.

The alarm priority for the guard tour events must be configurable.

User configurable instructions shall be available to assist operators when a guard tour alarm occurs.

The ISMS shall have an option to determine whether the guard must badge and open a door for a guard tour check point, or just present their card at the check point and not enter.

The ISMS shall be able to send an email and/or SMS alert to selected personnel based on guard tour events:

- it shall be possible to configure which events send alerts,
- it shall be possible to schedule when these alerts are sent.

The guard tour shall display in real-time the following information:

-
- the name of the guard,
 - the list of check points,
 - the time the guard is expected at each check point. This time shall display the deviation to indicate the time period the guard has to arrive at the check point.
 - This time period should update dynamically depending on the time the guard arrived at each check point.

The time the guard arrives at the check point.

The guard tour status should indicate (but not be limited to) the following:

- not due,
- due,
- early,
- overdue.

The guard tour shall stop if the guard arrives at an incorrect check point and an alarm shall be raised to indicate this.

The ISMS shall be configurable to restrict the individual guard tours that an operator can view.

The ISMS shall be configurable to determine whether an operator can view, edit or delete selected guard tours.

It shall be possible to display the real-time status of guard tours on a site map.

The guard tours shall be able to be started and stopped from the site map.

A site map showing the route of the guard tour shall be displayed.

It shall be possible to print a guard tour report directly from the site map.

The reports shall be configurable to filter based on the following criteria:

- date/time,
- guard tour,
- guard.

23. REPORTS

The ISMS shall provide report generation capabilities from the following sources of information:

- system activity data,
- cardholder access data,

-
- cardholder data fields,
 - cardholder access rights,
 - site configuration and setup data,

The report generation feature shall be easy to use and based on a “checkbox” style of parameter selection and preparation. The report preparation process shall provide features to simplify report generation by incorporating time selections such as “yesterday”, “last week”, “last month” etc. When these time-based selections are used in a saved report it will dynamically produce a report relevant to the time the report is run.

Report cover page, header, and footer, shall be configurable per report.

It shall be possible to re-order report columns.

It shall be possible to resize report columns.

The parameters for producing the report must be fully user definable and must be capable of searching on any cardholder or event criteria.

It shall be possible to produce the following types of reports:

- any site activity,
- last known location of all cardholders on site, with cardholder count summary,
- unprocessed alarms, un-acknowledged alarms and doors temporarily overridden from secure to free,
- details pertaining to cardholders, including images,
- time-and-attendance based reports.

Reports shall be able to be saved for future use.

There shall be no limit imposed on the number of reports that can be saved.

It shall be possible to copy a report to be used as a template for another report.

The report shall be generated by any of the following means, as may be required by the operator:

- within the report editor,
- manually triggered from within a map display,
- triggered by a hardware or software event,
- a one-time or recurring schedule.

The ISMS shall generate and format reports as a background process. This means the operator must be able to process alarms, alter database parameters and perform other system changes while the report is being generated. Report generation must continue if the operator decides to perform any other task.

The ISMS shall have a screen preview function, so that reports can be previewed during report preparation and on-screen before they are printed.

The report generator shall be capable of exporting reports in the following formats:

- Adobe PDF (.PDF),
- Microsoft Word (.DOCX),
- Microsoft XPS (.XPS),
- Microsoft Excel (.XLSX),
- image file (.JPEG),
- CSV file with header (.CSV),
- CSV file without header (.CSV).

It shall be possible to email reports to nominated people or groups of people using the above format.

The email capability shall be available from within the ISMS itself. Applications that require reports to be generated, saved to a file and then emailed using an external email application will not be acceptable.

The report generator shall be capable of supporting wildcard searching when filtering data for reports.

It shall be possible for operators to change report parameters when generating reports.

Reports shall be able to be printed at any network-supported printers connected to the ISMS.

The ISMS shall be able to produce voltage reports for a networked energised fence.

- The energised fence voltage reports shall be displayed in graphical form showing the energised fence voltage along with the date and time.

The ISMS shall be able to produce temperature reports for a networked energised fence controller.

- The networked energised fence controller temperature voltage reports shall be displayed in graphical form showing the energised fence controller temperature along with the date and time

Operator privileges shall differentiate between:

- report preparation and configuration,
- report generation only (not allowed to change the configuration).

It shall be possible to generate reports with graphical representations of data for trend analysis in the following formats:

- bar graph,

-
- pie graphs,
 - line graphs,
 - summary report data shall be available in a table format.

ISMS shall be able to change the start of the reporting week as required

24. NOTIFICATIONS

Specific event and alarm messages shall be able to be configured to be sent to nominated users via either email, SMS message, or mobile device application.

It shall be possible for persons receiving alarm messages to be able to acknowledge the alarms via return email or SMS message.

It shall be possible to send notification of imminent card or competency expiry to an individual, their manager or other nominated person.

When emailing cardholder details, it shall be possible to send an image of the cardholder from their personal data record.

A comprehensive filtering feature shall be provided to manage notification information transmission.

It shall be possible to schedule the notifications.

The notification may be triggered via a pre-configured alarm condition removing the need for operator intervention.

25. BULK NOTIFICATIONS

The ISMS shall allow for the broadcasting of notification messages to multiple recipients directly from the server.

The privilege to send the notification must be separate from the permission to create and see the setup of the notification.

Preconfigured messages shall be created that may then be sent with a single action by an operator or as a system triggered message.

The notification may be sent to groups filtered by previous access time, cardholder creation or modification date, access card type, or specific cardholder data criteria.

Notifications shall have the ability to be sent to dynamically updated groups based upon cardholder location in the ISMS.

26. AUDIT TRAIL

The ISMS server hard disk shall be used to record all system activity for auditing purposes.

All system activity event along with all details, including but not limited to the following list, shall be time stamped with the time of occurrence at the IFC and also the time the event was received by the server, to the nearest second, and shall be recorded in the system activity log for archiving:

- all access attempts (allowed and disallowed),
- alarm events,
- system events,
- operator activity.

The central control shall provide a facility to archive system data and event records to an archive file to free database space for further activity logging.

It shall be possible to archive the data to a network device by specifying a UNC path.

The archive process shall be initiated by either manual operation or automatically on a schedule.

It shall be possible to nominate the number of days of data that shall remain in the database after an archive process.

The ISMS reporting functionality shall return results from both live database and archive as a single contiguous report.

The system shall allow the workstations to acquire on demand subscriptions to the following and terminate these subscriptions after 5 minutes of inactivity

- Event Viewer
- Event Trail title
- Event Trail title

27. MOBILE DEVICE APPLICATION

The ISMS shall have a mobile device application which allows operators to remotely manage the ISMS via a smart phone or tablet. Dedicated devices with a single hardware option shall not be acceptable.

The mobile device application must be available on both Android and iOS operating systems.

The mobile device shall connect to the ISMS via:

- Wi-Fi or,
- mobile carrier data connection.

Mobile devices shall be enrolled in the ISMS by way of an authorisation code generated on the ISMS.

The mobile device connection must have the option of connecting to the ISMS server via an HTTPS proxy.

It shall be possible for the mobile device screen to lock after a preconfigured period of inactivity.

The mobile device shall be able to manage ISMS alarms:

- Alarms shall be displayed in different colours to denote the priority.
- The alarms shall have a flashing indicator when unacknowledged.
- The alarms will have a constant colour indicator when acknowledged.
- When multiple instances of the same alarm occur within a user-defined time frame, the mobile device will present alarms as a group and display the number of alarms in each group.
- The application will display the following alarm status:
 - alarm condition is still in an active state,
 - alarm priority has been escalated,
 - multiple occurrences of the same alarm within a user-defined time frame.
- The mobile device operator will be able to view alarm details such as:
 - priority,
 - source of the alarm,
 - date and time,
 - alarm history,
 - contextual instructions on how to proceed resolving the alarm.
- The mobile device operator will be able to perform operations on the alarm such as:
 - add notes to the alarm,
 - acknowledge alarms,
 - process alarms.
- The mobile device operator will be able to filter alarms by (but not limited to) the following states:
 - priority,
 - acknowledged,
 - unacknowledged,
 - active,

-
- inactive,
 - division.

The mobile device shall be capable of monitoring the status of ISMS items such as (but not limited to):

- doors,
- access zones,
- alarm zones,
- fence zones,
- macros.

It shall be possible to search for items monitored by the mobile device by selecting from a list or entering part of the text relating to the item name.

The mobile device shall be able to override items such as (but not limited to):

- doors,
- access zones,
- alarm zones,
- fence zones,
- macros.

The mobile device shall be able to lock down an access zone such that all cardholder access is disabled, excluding specifically authorised cardholders.

The mobile device shall have the capability to display the individual cardholders that are located in any access zone configured on the ISMS server.

The mobile device application shall have the ability to read Mifare DESFire EV2 credentials using the native NFC antenna of the mobile device.

- It shall be possible for the mobile application using NFC antenna to log a cardholder into or out of an access zone in the same manner as if the cardholder presented their card to a fixed access control reader.
- The cardholder credentials shall be authenticated by the ISMS and displayed in the user interface, clearly indicating an access granted or denied decision.
- Access granted and denied decisions shall be indicated by different audio tones.
- It shall be possible to continuously read cards without pressing any additional "Read Card" buttons.

The mobile device shall be able to manage cardholders.

-
- It shall be possible to search for cardholders by selecting from a list or entering part of the text relating to the cardholder's name.
 - It shall be possible to search for cardholders based on (but not limited to):
 - card number,
 - user defined data fields such as company, department, employee ID number, licence plate etc.
 - The mobile device shall display (but not be limited to) the following cardholder information:
 - name,
 - the last entered access zone, including date/time,
 - image,
 - access groups,
 - user defined data fields,
 - access credentials.
 - Data fields such as email address, phone number etc. shall be hyperlinks to enable the operator to click on the field and automatically be taken to the default email or phone application.
 - If a cardholder is not authorised for access, or has no active access groups, or has no active token, a highlighted message shall appear on the screen to alert the operator.
 - It shall be possible to disable a cardholder's access via the mobile device.

The mobile device shall be able to validate a searched for cardholder:

- It shall be possible to conduct a spot check of cardholders whereby the operator can view the access credentials of the cardholder on the Mobile device and record whether the cardholder passes an ID check and has the appropriate access rights to their current location.
- The operator shall select a "Pass" or "Fail" which will be logged at the central server.
- It shall be possible for the operator to select user-definable reasons for the pass or fail.
- It shall be possible for the operator to enter free text into a notes field.
- It shall be possible to record the location of the mobile device to indicate where the spot check took place.

The mobile device shall be capable of reading barcodes.

-
- Upon reading a barcode, it shall search for, and display cardholder details based on the barcode identifier.
 - The barcode identifier associated with the cardholder must support alpha-numeric characters. Numeric only will not be accepted.
 - The mobile device shall be capable of reading (but not limited to) the following barcode formats:
 - Aztec Code 2D,
 - DataMatrix 2D,
 - PDF417 2D,
 - QR Code 2D,
 - Macro PDF417 2D,
 - Semacode 2D.

The mobile device shall be capable of reading supported cards

ISMS shall allow the mobile version of the application to connect securely from anywhere on the internet hence removing the need for the mobile end point to be on a VPN or corporate network.

The mobile application shall display a selected profile image for cardholders who have been assigned this feature.

28. COMPETENCIES

Competencies shall be cardholder-based assignable attributes, used to determine if the cardholder is allowed access to specified areas based on factors relevant to the cardholder. The factors may be based on authority, or skill levels, or similar.

Multiple competency attributes may be assigned to one or more cardholder records.

Each competency will assume one of 4 different states:

- Active - The competency is currently valid for the cardholder.
- Expiry due - The competency is currently valid for the cardholder but will expire in a specified period.
- Expired - The competency has been assigned to the cardholder but has expired.
- Disabled - The competency, is temporarily disabled (or overridden) for the cardholder.

The competency states shall be configurable as “soft” - allowing access but generating an alarm; or “hard” - denying access, should a competency requirement not be met.

Each competency shall be individually set per cardholder

A field shall be provided to store the reason for disabling a competency.

Competencies shall be configured as required per access zone.

It shall be possible to exempt specific access groups from the requirement to meet specific competencies.

Denied access due to an invalid or missing competency shall be displayed to the user at the door reader.

Access permission based on competency criteria must be determined at the IFC, independent of the ISMS being on-line.

The reason for denied access due to an invalid competency shall be displayed on the door reader or keypad.

Advance warning of a cardholder's competency about to expire shall be sent to the individual and/or other nominated persons via email.

A consolidated report detailing competency expiry warnings for cardholders shall be sent via email to the associated manager.

29. RANDOM SELECTION

The ISMS shall have an integrated component for selecting cardholders using a completely random or pseudo-random criteria when they badge at a door.

The ISMS shall display a customisable message at a door's reader when the cardholder is selected.

The ISMS shall allow for configurable allowance or denial of access when the cardholder is selected.

The selection criteria shall be configurable with the following options:

- the maximum number of times that a single cardholder may be selected over a given period of time,
- the total number of cardholders that may be selected over a given period of time,
- that all cardholders must be selected at least once over a period of time.

The selection algorithm must be able to function on the IFC without the aid of the ISMS server.

The selection algorithm must be able to calculate the selection criteria across up to 30 doors in the system.

The selection algorithm must be able to differentiate between different groups of cardholders and assign a varying probability selection to each.

30. ELEVATOR CONTROL AND MANAGEMENT

The ISMS shall provide fully integrated elevator control facilities. The elevator control access equipment must communicate with the same central control as the door card readers.

The elevator control architecture shall comprise a card reader in each elevator car, reporting to elevator control interface equipment mounted in or near the elevator motor room. Reader type shall be as specified for use on access control doors.

The elevator control system shall be capable of controlling access independently in a number of elevator shafts simultaneously.

The elevator control system shall incorporate dedicated intelligence and a local database of authorised cardholders.

Each elevator reader shall be identified independently at the central control by means of a unique plain language descriptor. The central control plain language descriptor shall be at least 60 characters in length.

The ISMS shall raise an alarm if the elevator reader stops communicating with its elevator controller.

The elevator control shall check entry based on all of the following criteria:

- correct facility code,
- authorised card in database,
- correct issue number,
- authorised level,
- authorised time of day,
- correct PIN (If PIN entry is required).

The access mode for each floor of an elevator shall be capable of automatically changing according to the programmed time schedules, as received from the central control. The following access criteria modes are required:

- free access (no credential required),
- secure access (credential required),
- secure and PIN access (credential and PIN required),
- dual authorisation - access is granted when two different but legitimate cards are presented within a given time frame,
- escort - a second card is required to be presented from a cardholder who is nominated in a specified access group,
- shared code - The ISMS operator determines what the code will be and programs this into the ISMS. Access is allowed through the elevator when the correct 4-digit code is entered.

Levels must be securable on a level by level basis, using command instructions transmitted from the central control.

The central control must provide operator override facilities to enable temporary override capability on a level by level basis.

Where a low-level interface is specified:

- The interface between the access system elevator control equipment and the elevator switching control equipment shall be via dry relay contacts.
- The voltage from the elevator system connected to the relays shall not exceed 24 volts DC/AC.
- The elevator control system shall provide one relay contact per elevator shaft per level for the ISMS. This relay contact shall be used to interface with the elevator switching control equipment.
- An input shall be provided for each level per elevator to indicate what level the user selected. On activation of this input all relays return to secure state.

Where a high-level interface is specified:

- The interface between the access system elevator control equipment and the elevator switching control equipment shall be via RS-232 or TCP/IP connection depending in the elevator system requirements.
- The elevator control equipment will provide feedback as to which level was selected by the cardholder.

31. CAR PARKING

The ISMS shall integrate car park management functionality.

Car parks may be allocated to a single cardholder or a group of cardholders.

Car park functionality for a group of cardholders:

- When occupancy of a group's car parks is reached the system shall disallow entry to members of that group until another group member has left the car parking area.
- The car parking functionality may allow for a cardholder to enter the parking area temporarily although there are no available parks for their group to ensure they do not cause a traffic jam at the entry point.
- If the cardholder that was allowed temporary entry does not leave the car park area after a configured period of time, then an alarm shall be raised in the ISMS.
- If another member of the parking group leaves the car park, then this shall allow the cardholder with temporary entry to remain in the car park.

The ISMS shall provide a real-time display to show the current occupancy of car parks.

The car parking system shall use standard readers and i/o devices to interface to barrier arms.

There shall be a terminal provided that gives feedback to a cardholder at the time of credential presentation.

The car parking system shall support all credentials specified in this tender including Bluetooth.

32. LOCKER SYSTEM

The ISMS shall include a locker management solution.

The lockers shall have the ability to be dedicated to a single person or allocated on-demand via a terminal when needed.

On-demand allocation of lockers shall not be reliant upon the ISMS server.

The lockers shall be able to be configured as either having an expiry period, or permanently assigned.

A quarantine state shall be configurable:

- To automatically occur when a locker allocation expires.
- With manual override for maintenance purposes.

The locker management system shall use standard readers and i/o devices to interface to locker bank hardware.

There shall be a terminal provided that gives feedback to a cardholder as to which locker they have been provided at the time of credential presentation.

A single terminal shall be able to support up to 256 lockers.

There shall be no limit to the total number of lockers in the system.

The locker management system shall support all credentials specified in this tender including Bluetooth.

33. PRE-PROGRAMMED OVERRIDE MACROS

To allow for making changes to the ISMS configuration on demand, it shall be possible to pre-configure the required changes and assign them to a macro action.

Macro actions shall be capable of (but not limited to) the following:

- open doors,
- change door modes such as free, secure, secure with PIN, dual authority,
- anti-passback forgive,
- active and release zone lock down,

-
- reset the cardholder count in a zone,
 - switch an output on and off,
 - activate the generation of pre-configured reports,
 - start and stop a guard tour,
 - initiating another macro.

A macro shall be capable of activating multiple actions from within a single macro. There shall be no fixed limit to the number of actions that can be configured.

An operator shall be able to initiate the macro via either a menu item or by a site plan icon.

Macros shall be capable of being activated by any ISMS events.

Macro configuration must be by the use of GUI features such as drop-down lists and drag and drop techniques. The use of script language to write macros is not acceptable.

It shall be possible to initiate macros based on a on a time schedule.

Macros shall be able to execute Microsoft Windows command line actions.

Up to 300-character variables shall be able to be specified for each command line.

Each macro shall be able to contain multiple command line entries.

The configuration and execution of command line macros shall be user account name and password protected. These usernames and passwords shall be obscured on entry and transmitted and stored at the central command ISMS server in an encrypted format.

34. VISITOR MANAGEMENT KIOSK

The ISMS shall allow visitors to self-register as defined in this section.

The kiosk shall operate on a workstation provided to the specification defined in “System Servers and Workstation Hardware”.

The kiosk shall support touch screen functionality.

Visitor personal details shall be stored if required, to be reused for future visits.

Visit details shall be recorded in the ISMS event database.

Attributes associated with the visit shall be configurable and set as mandatory or optional fields. These shall include:

- the reception where the visitor(s) will be expected to arrive,
- the visitor category,
- the person the visitor(s) will be meeting,
- visitor arrival time,

-
- visitor departure time,
 - building access rights to be given to the visitor(s),
 - visitor photo-ID image.

Visitor details for several visitors associated with a single visit shall be able to be pre-registered into the ISMS.

A welcome (default) screen shall be customer configurable to allow branding and imagery to be displayed.

The kiosk shall support visitor site induction.

- The induction feature shall be customer configurable, incorporating the following features:
 - induction videos,
 - multi-choice questionnaire depending on induction level required,
 - multiple questionnaires,
 - induction hint feature to allow the visitor to request a hint for questions,
 - notify the host that the visitor requires induction assistance,
 - a condition of entry screen,
 - a privacy statement screen.

Visitors shall be able to search for themselves in the system and carry out the following functions:

- add or update their details,
- capture a photograph via a camera connected to the kiosk,

The ISMS shall raise an alarm should a visitor not sign out by the due time.

If the visitor has been assigned an access token, then the visitor shall be able to present their token as identification.

The kiosk shall support business card scanning via a Dymo Executive Business Card Scanner.

The kiosk shall support passport and driver licence scanning via ScanShell products.

For pre-arranged visits, the visitor shall be able to pick the visit from a drop-down list.

The visitor shall be allowed to print a visitor label.

Visitors shall be able to advise their host via the ISMS that they have arrived via email or SMS message.

Hosts shall be able to assign themselves to the visitor by badging at a Card Reader.

Hosts shall be able to set the status of visitors to ensure current status of each visitor is always known. Host options shall include:

- marking a visitor on or off site,
- reprinting a badge for a visitor,
- updating visitor details such as arrival and departure times,
- assigning an access card to the visitor.

Tour groups shall be catered for.

- Tour group members are not individually named, however the number of people in the group shall be recorded.

Groups of visitors shall be selectable as a group and their status processed as a single action.

The kiosk shall support a QR Code scanner.

- Upon creating an appointment, the visitor may be emailed a QR code which can be used to sign in.
- The QR code if used for signing in shall also be used for signing out.

35. DOOR FUNCTIONALITY – CONNECTED TO CONTROLLER

Access control for a door shall allow for the following features where specified:

- access reader,
- emergency release switch input,
- reception control switch input.

Egress control for a door shall allow for the following features where specified:

- exit reader,
- push button request to exit,
- emergency exit break-glass.

A push button request to exit shall record the exit in the event database.

When requested by a valid means of access or egress, the door shall unlock for a preset period, after which the door shall relock.

- The door relock time shall support three modes of operation:
 - the door lock output will relock immediately on door open
 - the door lock output will relock after a door open/close cycle

-
- the door lock output will relock after the configured time regardless of open-close cycles
 - The period of unlock shall be extended should a cardholder have a suitable privilege.

All entry and exit methods shall be recorded in the event in the event database.

The door shall be monitored for both door open/closed, and door locked/unlocked using concealed monitor switches appropriate for the door installation.

Where the door is a double door, the inactive door leaf shall also be monitored for door open/closed and door unlocked/locked. The inactive leaf door monitor switches may be connected as part of the active door leaf monitoring.

It shall be possible to configure the door in a way that generates a forced door alarm should the door be unlocked and/or opened without first being released by the ISMS.

Should a door be left unlocked or open after a preset time, an alarm shall be generated reporting the condition.

The door open/unlocked warnings shall provide an audible warning at the door.

It shall be possible to disable the reader audible warning.

It shall be possible to generate the audible warning via a relay connected elsewhere in the ISMS including any other IFC.

Should a valid request to access a door be generated and access not taken, this will be recorded as a different event and the door will be re-secured.

The ISMS shall have a lock down feature whereby cardholders who would usually have access to doors are denied access.

- It shall be possible to assign specific cardholders the right to access a door when the door is in lock down, whilst refusing access to all other cardholders.

It shall be possible to create an interlock relationship between groups of doors for situations such as airlocks whereby a door cannot be opened until other doors or inputs are closed.

- Up to 20 doors shall be included in any interlock group.
- It shall be possible to configure interlock groups via GUI drag and drop functionality without the requirement to write scripted logic.
- It shall be possible to assign outputs that advise cardholders that there is an interlocked state active.

The ISMS shall support a challenge or video verification mode as specified below:

- When a card is presented at a reader, images from the cardholder database (as many as required) shall be displayed in the challenge view of an operator GUI.

-
- Associated with the images, it shall be possible to display a video image from one or more assigned cameras.
 - In challenge mode it shall be possible to view a site plan showing the location and status of the controlled entry point and nearby items.
 - In challenge mode it shall be possible for the operator to view the status of the cardholder's cards and competencies for informing the cardholder, at the time of entry, if any expiries are imminent.
 - Related data fields shall also be able to be displayed, associated with the cardholder (name details, department etc).
 - Associated with a challenge entry, the selection and layout on screen of cardholder images, cardholder personal data, cardholder card or competency status, site plans or video images must be configurable using simple drag and drop, or click and drag techniques to resize or reposition information.
 - The challenge mode shall be configurable to either:
 - Automatically grant access to a valid card and display the current access decision (granted or denied) to the challenge operator.
 - Require operator intervention to grant access to a valid cardholder.
 - Should a second challenge be requested while an unanswered challenge remains in the ISMS, the second and subsequent challenges shall queue automatically awaiting response.
 - It shall be possible for an operator to view waiting challenge events and to select and process challenge events within the queue in any order they choose.
 - The ISMS shall allow challenge events to be managed from a single full-screen view per operator or multiple filtered views, as dictated by the specification.

36. DOOR FUNCTIONALITY – DATA ON CARD

Where specified, doors shall be managed using an offline door locking system.

A single interface shall be provided that allows for administration and reporting including both the online and offline locking systems.

The offline doors shall be fully integrated into the ISMS as described below:

- Card technology shall be contactless Mifare Classic, Mifare Plus, or Mifare DESFire EV2.
- Card encoding shall be carried out as a single encode operation for both online and offline door readers.
- Operational data shall be transferred between the ISMS and offline doors automatically, without the need for specific operator actions. This data shall include:

-
- multiple levels of door low battery voltage alarms,
 - access activity from all doors,
 - blacklisted card information,
 - changes to cardholder access privileges.
- Access privileges based on time and day shall be available, with full flexibility in specifying the time intervals or day types for any cardholder.
 - It shall be possible to configure the ISMS to ensure access updates for offline doors are enforced within a given period of time, configurable as a minimum of 1 day.
 - Access privilege changes must not require connection of a management device to the escutcheon (eliminating the need to update each door escutcheon when a user is added or removed).
 - The ability to specify an extended door opening time for specific cardholders shall also be available for offline doors.
 - Offline doors shall support partitioning to allow specific administrators to control and assign access privileges within their own environment/facility.

The range of hardware shall include an option for an internal privacy lock which, when activated, prevents entry except for privileged users.

Hardware shall not use proprietary batteries. Batteries must be commonly available types.

Battery life shall support a minimum of 35,000 operations before replacement is required.

The escutcheon hardware shall be compatible with the lock hardware specified for this project.

Basic maintenance (changing batteries, changing basic configuration) shall be able to be carried out by general maintenance staff with minimal instruction.

The offline escutcheons should be able to hold an audit trail of at minimum the last 1000 events.

The offline escutcheons shall be able to function in a variety of modes such as but not limited to, free (unlocked), secure (locked) by schedule or as controlled by a cardholder with privilege to change the escutcheon mode.

It shall be possible to change a door state between the free and secure states using an authorised card.

It shall be possible to specify on a user by user basis what modes they can place the lock in (e.g. free or secure) and override functions the user can perform (i.e. entry allowed when privacy lock is on).

A handheld programming device may be used for the purposes of:

- diagnosing problems,

-
- performing an emergency opening of an offline escutcheon,
 - updating software,
 - provide power to the escutcheon to allow resolving a no battery voltage situation,
 - initialising hardware.

Multiple levels of warning for low battery indication including audible, visual and physical warnings (i.e. initially a visual signal progressing to an audible and visual indicator and then finally progressing to an audible, visual and delayed opening of the door to indicate/prompt someone to report the occurrence). One or all may be used.

The hardware range shall include the ability to upgrade offline doors to online via wireless through a wireless gateway.

37. DOOR FUNCTIONALITY – WIRELESS CONNECTIVITY

Where specified, doors shall be managed using an escutcheon based, wireless door locking system.

A single, seamless user interface shall be provided within the head end to ensure integrity of access decisions are maintained within the primary access control system.

The flow of information from the RFID card shall be transmitted instantaneously to the wireless card reader/lock, (escutcheon or cylinder type) which shall in turn send the card credentials to the hub and access control system.

The ISMS shall provide real-time access decisions as described elsewhere in this specification.

Assignment of access privileges for use in both online and wireless doors shall be available through a single interface.

Card encoding shall be carried out as a single encode operation for both online and wireless door readers

A wireless RS485 communication hub shall support up to 8 wireless escutcheons or cylinders and have reliable communication to each reader within 15 metres.

- Wireless hubs shall be able to be wired in series with RS485 compatible cable.
- The wireless hub shall conform to the radio standard applicable to the region of installation and conform to IEEE802.15.4 (2400 – 2483.5 MHz).
- AES-128 encryption shall apply for communication between the hub and each wireless reader.
- Up to 16 (installer selectable) channels per hub shall be available to ensure each wireless escutcheon or cylinder is configured with reliable communication.
- Hardware shall not use proprietary batteries. Batteries must be commonly available types.

-
- Battery life shall support a minimum of 35,000 operations before replacement is required.

The wireless doors shall be fully integrated into the ISMS as described below:

- Card technology shall be contactless Mifare Classic, Mifare Plus, or Mifare DES-Fire EV2.
- Operational data shall be transferred between the ISMS and wireless doors automatically, without the need for specific operator actions. This data shall include:
 - multiple levels of door low battery voltage alarms,
 - access activity,
 - blacklisted card information,
 - changes to cardholder access privileges.

The escutcheon hardware shall be compatible with the lock hardware specified for this project.

Basic maintenance (changing batteries, changing basic configuration) shall be able to be carried out by general maintenance staff with minimal instruction.

An installer service tool shall communicate with each wireless hub and enable configuration, management, and override of each door independent of the access control system.

38. FIELD HARDWARE – INTELLIGENT FIELD CONTROLLER (IFC)

The IFC shall be the main controller in the field. The ISMS shall communicate directly with all IFCs.

The IFC shall use a Linux operating system, this OS shall be specifically re-developed for a security purpose. Applications on a general-purpose OS such as Windows CE, Arduino, or a standard Linux kernel shall not be accepted.

The IFC shall incorporate an ARM processor with a processing speed of at least 1.2GHz; at least 4 Gigabytes of non-volatile FLASH eMMC and 512 Megabytes of RAM. The IFC shall incorporate boot code in a protected sector of the flash memory.

During IFC firmware upgrades, this shall be checked and verified as the true firmware pack during the upgrade process.

The IFC shall be intelligent such that in the event of failure of communications to the ISMS, for whatever reason, the IFC shall continue to allow or deny access based on the full security criteria at time of disconnection.

The IFC shall store on-board all the security and access parameters to operate completely independently from the central control server. Systems that rely on the central control server for access decisions will not be considered.

The IFC shall buffer activity data and immediately transmit it to the central control server upon re-establishment of communications.

Should communications fail with the ISMS, each IFC shall be capable of buffering up to 1,000,000 events.

All events shall be time-stamped at the IFC at the time of occurrence.

ISMS that only time stamp the event upon receipt at the central control hardware shall not be acceptable.

The IFC shall be capable of storing up to 2,000,000 card records with associated access criteria.

The IFC shall be capable of storing up to 1,000,000 mobile credentials with associated access criteria.

The IFC shall be capable of storing up to 1,000,000 biometric credentials with associated access criteria.

The IFC shall support the use of six-state end-of-line circuits and enunciate whether the circuit is open, closed, alarm, trouble, open circuit tampered, or short circuit tampered as separate conditions.

A configurable range of end-of-line resistor values shall be supported as a software function to support pre-existing input circuits when required.

The IFC shall include tamper protection for the front and the back of the unit. The front of the unit shall be tamper protected for enclosure open, and the rear of the unit to detect if the unit has been removed from the wall.

The IFC shall operate from a DC power source with battery backup.

IFC's shall have power source options that enable:

- DC power supply with standby power at the power source.
- Power over Ethernet (802.3at Type 2 compliant) and must have a capability to maintain a 7Ah battery for standby power.
- Automatic detection and reporting of a PoE loss.

The IFC shall be capable of automatically detecting and reporting a low power condition.

IFCs shall automatically restart and resume processing following a power failure.

IFCs shall be fitted with "watchdog" software to provide automatic detection and restart should the processor lock up.

The IFC shall contain its own real-time clock. The clock shall be synchronised with the central control server clock at least once per hour. The accuracy shall be such that the time difference between IFCs shall not vary more than 0.5 second at any time.

The IFC shall be allocated to a time zone appropriate to the IFC location to cater for regionally and globally located IFCs.

When specified, the IFC shall support 100/1000BaseT.

When specified, the IFC shall be fitted with 2 Ethernet ports providing a fail-over communication capability.

The IFC shall have IPv6 address support.

The IFC shall support DHCP addressing.

The IFC shall be able to automatically obtain an IP address from a standard DHCP server.

The ISMS shall natively support WAN and NAT configurations to communicate with IFCs on distributed networks.

The IFC shall support DNS operation.

Should the primary DNS not be available, the IFC shall be able to automatically establish contact with a secondary or tertiary DNS.

The IFC shall be provided with a pre-configured IP address to allow offline initial configuration via a web browser application when required.

It shall be possible to view the IFC status and configuration for commissioning and diagnostic purposes without the use of the central server software or other proprietary software. This may be achieved using a conventional web browser.

The IFC diagnostic web interface shall:

- Not share common log on credentials with any other installed site.
- Have the ability to be disabled from the ISMS system.

Should excessive network broadcast traffic occur (resulting from a denial-of-service attack or similar), an alarm shall be generated.

The IFC shall support a high security configuration that disables unnecessary ports and legacy communication methods, this shall be achieved by an onboard jumper or DIP switch.

All ISMS data communication between the central server and IFCs shall be fully authenticated and encrypted using an industry standard asymmetric encryption algorithm equivalent to AES-256 or stronger.

All data communication between IFCs, IFCs and ISMS shall use an industry standard asymmetric encryption algorithm for mutual authentication and session key negotiation. This algorithm shall be equivalent to ECC P-384 or stronger. Session keys shall be re-negotiated on a regular basis at intervals no longer than 30 hours.

The IFC shall store and encrypt its cryptographic keys within its dedicated hardware for protection.

The IFC shall use Trusted Execution Environment (TEE) based on the ARM Platform Security Architecture.

Data onboard the IFC shall be encrypted at rest to prevent unauthorised access.

Communication between the management application and IFCs shall be continuous and monitored for interruption.

IFC variants shall enable remote communication to alarm monitoring stations with connection options:

- RS232 multi-communication port.
- TCP/IP for alarm transmission.

The IFC shall support logic functionality by way of configurable logic blocks.

- The IFC logic functionality shall be able to be run independent of the ISMS server being online.
- The following items shall be useable as input parameters to logic blocks:
 - physical input states,
 - output states (both physical and logical),
 - door states,
 - other logic block states.
- Up to ten logic block input parameters shall be configurable in AND/OR combinations to cause a logic block to operate.
- When a logic block change state according to the input parameters then the following types of items may change to reflect the state of the logic block:
 - virtual output (software based),
 - physical relay.
- The state change of the logic block shall have configurable timing options with at least the following:
 - explicit,
 - delay on,
 - delay off,
 - pulsed,
 - maximum on time,
 - latched.
- The IFC logic block shall be able to trigger actions across multiple IFCs, independent of the ISMS server being online.

A separate alarm message shall be transmitted to the ISMS for at least the following alarm conditions. The alarm message shall be displayed in plain language text.

- tamper,

-
- tamper return to normal,
 - unit stopped responding,
 - card error,
 - maintenance warning,
 - alarm sector state change,
 - user set alarm,
 - user unset alarm,
 - card trace,
 - wrong PIN,
 - access denied,
 - duress,
 - zone count maximum,
 - zone count minimum,
 - door open too long,
 - forced door,
 - door not locked,
 - power failure,
 - battery failure,
 - system reboot,
 - intercom.

The IFC shall communicate with and control the following equipment:

- biometric access readers,
- card access readers with PIN keypads,
- elevator access equipment,
- alarm monitoring input/output panels and equipment,
- alarm response equipment.

All communications links between the IFCs and remote devices shall be monitored such that an alarm is raised at the central control if the data being transmitted is corrupted or tampered with in any way.

Communication between IFCs and downstream devices shall support a high-speed serial protocol of at least 1Mbit/second.

IFC variants shall support up to 10 high speed serial communication ports.

The IFC shall support up 80 devices comprising a combination of readers, I/O devices and sensors.

Devices connected to the high-speed communication serial port shall contain a manufacturer's unique serial number.

When connected to an IFC, the serial number of the downstream device shall be reported to the ISMS.

Once assigned to a function within an IFC, if any attempt is made to substitute readers in the field without authorisation, an alarm shall be generated.

The IFC shall have OSDP reader support.

The IFC shall provide relay output facilities that are activated in response to alarm activations. Relay functions required are:

- Activate and latch a relay in response to an alarm. Relay to remain latched until alarm processed.
- Activate a relay for pre-set "pulse" time. The relay to release after the "pulse" time lapses.
- Relay activation to "mirror" or "follow" the alarm input activation.

The ISMS shall incorporate relay outputs that can be activated according to time schedules, rather than alarm event.

The IFC shall support direct third-party communications with:

- Building management systems
- 3rd party API systems
- High level interfaced elevator systems

The IFC must comply with in ceiling space/plenum installation standards.

The IFC shall meet Compliances

- UL294 – Level 3
- UL2610 – Proprietary, Centralised station, mercantile
- UL2043
- IEC/ASNZS 60839-11-1
- ASNZS 2201.1
- EN BS50131

-
- FIPS 140-2 Level 3
 - CE/UKCA
 - FCC

39. ENCRYPTED END OF LINE DEVICE – CLASS 5

Encrypted end of line devices shall be available to provide secure monitoring of alarm inputs, i.e. passive infrared sensors, contacts.

The End of Line Device (ELD) must conform to the AS/NZS 2201 Class 5 Intruder Alarm Standard.

The ELD is required to fit securely inside the housing of a AS/NZS 2201 complaint PIR.

Alarm input devices must connect to the ISMS via an ELD.

The ELD must communicate with the ISMS using encrypted communications.

The ELD shall support the following I/O to the alarm device:

- alarm input,
- tamper input,
- anti-masking input,
- walk test output,
 - the walk test output shall support either a positive or negative output voltage during testing.

Events relating to the ELD shall be visible at the ISMS.

The ELD shall be encapsulated in a protective resin and plastic casing to prevent tampering.

The ELD shall support self-discovery on the ISMS.

The ELD shall be identifiable via a manufacturer's unique serial number both indelibly marked on the ELD and at the ISMS.

When connected to an IFC, the unique number of the ELD shall be reported to the ISMS.

The ELD is required to generate an alarm for the following conditions:

- attempted substitution of the ELD,
- external tamper sensor activated,
- communications lost to ISMS,
- alarm input triggered,
- anti-mask input triggered.

The ELD shall be upgradeable via software uploaded from the ISMS without any intervention at the ELD.

Each ELD shall be identified on the operator GUI by means of a user definable unique plain language descriptor. The plain language descriptor shall be at least 60 characters in length.

It shall be possible to connect up to thirty ELDs to a single IFC.

The ELD shall support a serial wiring configuration.

The ELD shall operate at temperatures between -10°C to +70°C

40. ENCRYPTED END OF LINE DEVICES

Encrypted end of line devices shall be available to provide secure monitoring of alarm inputs, i.e. passive infrared sensors, contacts.

The purpose of the ELD is to overcome the security weakness created by non-authenticated sensor inputs using a balanced resistor network.

The ELD shall be small enough to fit inside the housing of a PIR.

Alarm input devices must connect to the ISMS via an ELD.

The ELD must communicate with the ISMS using encrypted communications.

The ELD shall support the following I/O to the alarm device:

- alarm input,
- tamper input,
- anti-masking input,
- walk test output,
 - the walk test output shall support either a positive or negative output voltage during testing.

Events relating to the ELD shall be visible at the ISMS.

The ELD shall be encapsulated in a protective resin and plastic casing to prevent tampering.

The ELD shall support self-discovery on the ISMS.

The ELD shall be identifiable via a manufacturer's unique serial number both indelibly marked on the ELD and at the ISMS.

When connected to an IFC, the unique number of the ELD shall be reported to the ISMS.

The ELD is required to generate an alarm for the following conditions:

- attempted substitution of the ELD,

-
- external tamper sensor activated,
 - communications lost to ISMS,
 - alarm input triggered,
 - anti-mask input triggered.

The ELD shall be upgradeable via software uploaded from the ISMS without any intervention at the ELD.

Each ELD shall be identified on the operator GUI by means of a user definable unique plain language descriptor. The plain language descriptor shall be at least 60 characters in length.

Communication sessions between IFCs and ELDs shall use certificate exchange protocols using keys with a minimum strength of ECC P-256.

Data communication between IFCs and ELDs shall use a minimum of AES-128 encryption.

It shall be possible to connect up to thirty ELDs to a single IFC.

The ELD shall support a serial wiring configuration.

The ELD shall operate between -10°C to +70°C.

41. ACCESS CONTROL READERS – MIFARE TECHNOLOGY

The reader shall support the following technologies:

- Mifare Classic,
- Mifare Plus,
- Mifare DESFire EV1,
- Mifare DESFire EV2,
- NFC.

The reader shall be capable of reading the CSN of the Mifare card and store the CSN in the ISMS database

The readers shall support self-discovery on the ISMS.

- Readers shall contain a manufacturer's unique serial number.
- When connected to an IFC, the serial number of the reader shall be reported to the ISMS.
- Once assigned to a function within an IFC, if any attempt is made to substitute readers in the field without authorisation, an alarm shall be generated.

Data communication rate between IFCs and readers shall be at least 1Mbit/second.

Communication sessions between IFCs and readers shall use certificate exchange protocols using keys with a minimum strength of ECC P-256.

Data communication between IFCs and readers shall be encrypted and use a minimum of AES-128.

Readers shall generate a heartbeat signal to enable the IFC to identify lost communications and thereby generate an alarm.

Readers shall be upgradeable via software downloaded from the ISMS without any intervention at the reader.

The reader must accept a message from the IFC to advise that data from reader to IFC has been received and to consequently stop sending the card data.

Each reader shall be identified independently on the ISMS by means of a unique plain language descriptor. The plain language descriptor shall be at least 60 characters in length.

Where a card only reader is specified, the reader shall include:

- Integrated reader module supporting the technologies listed above.
- The card only reader option shall include an audible beeper and red/green LEDs to provide user feedback.
 - A steady red LED shall indicate door secure.
 - A flashing red LED shall indicate access denied.
 - A steady green LED shall indicate door free access.
 - A flashing green LED shall indicate access granted.
 - It shall be possible to turn off the reader LED indication via the ISMS software.
- The beeper shall give different beeps to indicate:
 - access granted,
 - access denied,
 - second card required when dual card authorisation or escort mode is programmed,
 - it shall be possible to turn off the reader beeper via the ISMS software.
- The readers must comply with at least IP68 environmental protection rating.
- The readers must comply with an impact rating of at least IK07
- A vandal resistant enclosure having an impact rating of at least IK08 rating shall be available where:

-
- Vandal covers shall be fixed to the wall surface using tamper-resistant screws.
 - Vandal covers shall have bevelled edges to limit the ability for persons to use the reader as an aid to climbing the building.
 - All external surfaces shall be bevelled and without protruding parts to meet anti-ligature requirements.
 - The reader must be RoHS compliant
 - The reader shall operate with a temperature range of -30°C to +70°C.

Where a PIN pad is specified, the reader shall include:

- integrated reader module supporting the technologies listed above,
- a minimum of a 3.5" LED colour display indicating:
 - card required,
 - PIN required,
 - access denied,
 - intruder alarm set,
 - intruder alarm unset,
 - free access,
 - second card required.
- The display shall support multiple languages which shall be selectable from the ISMS software.
- The reader shall display information to the user using a combination of text and graphics.
- The reader shall display the date and time.
- a PIN pad fully integrated with the reader,
- the PIN pad shall be backlit,
- The PIN pad shall include:
 - numerical 0 to 9 keys,
 - a cancel key,
 - an enter/accept key,
 - two soft keys that vary according to the current usage of the keypad.
 - An option with no reader module, for use as an AMT.

-
- Menus shall be accessible by logging on with either a card or a PIN.
 - The reader shall be capable of (but not limited to) carrying out the following functions:
 - Arm alarm zones; A minimum of 50 per reader must be supported.
 - Disarm alarm zones; A minimum of 50 per reader must be supported.
 - View Alarms; A minimum of 100 per reader must be supported.
 - Acknowledge alarms; A minimum of 100 per reader must be supported.
 - View alarm history; A minimum of 100 per reader must be supported.
 - Change the door to free access mode.
 - Change the door to secure access mode.
 - Change the door to operate from a user defined schedule.
 - Turn outputs on and off. A minimum of 50 per reader must be supported.
 - View the status of inputs. A minimum of 100 per reader must be supported.
 - Isolate inputs. A minimum of 100 per reader must be supported.
 - User definable custom images shall be displayed on the screen when the reader is idle.
 - The reader shall support the following image formats:
 - PNG,
 - JPG,
 - JPEG.
 - It shall be possible to adjust the reader beeper via the ISMS software to the following volume levels:
 - off,
 - quiet,
 - normal,
 - loud.
 - The reader shall have the ability to display the status of alarms and indicate the status of physical and logical items via LEDs on front panel.
 - The reader shall support at least 8 indication LEDs.
 - It shall be possible to turn off the reader indicator LEDs via the ISMS software.

-
- Tamper detection shall be provided against the unit being removed from the mounting surface.
 - Keypad readers must comply with a minimum IP66 environmental protection rating.
 - Keypad readers must comply with an impact rating of at least IK08.
 - The keypad reader shall operate with a temperature range of -30°C to +70°C.

All readers must be RoHS compliant.

42. ACCESS CONTROL READERS – MULTI TECHNOLOGY

The reader shall support the following technologies:

- Proximity 125 kHz
- Mifare Classic,
- Mifare Plus,
- Mifare DESFire EV1,
- Mifare DESFire EV2,
- NFC,
- Bluetooth LE.

The reader shall be capable of reading the CSN of the Mifare card and store the CSN in the ISMS database

The readers shall support self-discovery on the ISMS.

- Readers shall contain a manufacturer's unique serial number.
- When connected to an IFC, the serial number of the reader shall be reported to the ISMS.
- Once assigned to a function within an IFC, if any attempt is made to substitute readers in the field without authorisation, an alarm shall be generated.

Data communication rate between IFCs and readers shall be at least 1Mbit/second.

Communication sessions between IFCs and readers shall use certificate exchange protocols using keys with a minimum strength of ECC P-256.

Data communication between IFCs and readers shall be encrypted and use a minimum of AES-128.

Readers shall generate a heartbeat signal to enable the IFC to identify lost communications and thereby generate an alarm.

Readers shall be upgradeable via software downloaded from the ISMS without any intervention at the reader.

The reader must accept a message from the IFC to advise that data from reader to IFC has been received and to consequently stop sending the card data.

Each reader shall be identified independently on the ISMS by means of a unique plain language descriptor. The plain language descriptor shall be at least 60 characters in length.

Where a card only reader is specified, the reader shall include:

- Integrated reader module supporting the technologies listed above.
- The card only reader option shall include an audible beeper and red/green LEDs to provide user feedback.
 - A steady red LED shall indicate door secure.
 - A flashing red LED shall indicate access denied.
 - A steady green LED shall indicate door free access.
 - A flashing green LED shall indicate access granted.
 - It shall be possible to turn off the reader LED indication via the ISMS software.
- The beeper shall give different beeps to indicate:
 - access granted,
 - access denied,
 - second card required when dual card authorisation or escort mode is programmed,
 - it shall be possible to turn off the reader beeper via the ISMS software.
- The readers must comply with at least IP68 environmental protection rating.
- The readers must comply with an impact rating of at least IK07
- A vandal resistant enclosure having an impact rating of at least IK08 shall be available where:
 - Vandal covers shall be fixed to the wall surface using tamper-resistant screws.
 - Vandal covers shall have bevelled edges to limit the ability for persons to use the reader as an aid to climbing the building.
 - All external surfaces shall be bevelled and without protruding parts to meet anti-ligature requirements.
- The reader must be RoHS compliant

-
- The reader shall operate with a temperature range of -30°C to +70°C.

Where a PIN pad is specified, the reader shall include:

- integrated reader module supporting the technologies listed above,
- a minimum of a 3.5" LED colour display indicating:
 - card required,
 - PIN required,
 - access denied,
 - intruder alarm set,
 - intruder alarm unset,
 - free access,
 - second card required.
- The display shall support multiple languages which shall be selectable from the ISMS software.
- The reader shall display information to the user using a combination of text and graphics.
- The reader shall display the date and time.
- a PIN pad fully integrated with the reader,
- the PIN pad shall be backlit,
- The PIN pad shall include:
 - numerical 0 to 9 keys,
 - a cancel key,
 - an enter/accept key,
 - two soft keys that vary according to the current usage of the keypad.
- Menus shall be accessible by logging on with either a card or a PIN.
- The reader shall be capable of (but not limited to) carrying out the following functions:
 - Arm alarm zones; a minimum of 50 per reader must be supported.
 - Disarm alarm zones; a minimum of 50 per reader must be supported.
 - View alarms; a minimum of 100 per reader must be supported.
 - Acknowledge alarms; a minimum of 100 per reader must be supported.

-
- View alarm history; a minimum of 100 per reader must be supported.
 - Change the door to free access mode.
 - Change the door to secure access mode.
 - Change the door to operate from a user defined schedule.
 - Turn outputs on and off; a minimum of 50 per reader must be supported.
 - View the status of inputs; a minimum of 100 per reader must be supported.
 - Isolate inputs; a minimum of 100 per reader must be supported.
 - User definable custom images shall be displayed on the screen when the reader is idle.
 - The reader shall support the following image formats:
 - PNG,
 - JPG,
 - JPEG.
 - It shall be possible to adjust the reader beeper via the ISMS software to the following volume levels:
 - off,
 - quiet,
 - normal,
 - loud.
 - The reader shall have the ability to display the status of alarms and indicate the status of physical and logical items via LEDs on front panel.
 - The reader shall support at least 8 indication LEDs.
 - It shall be possible to turn off the reader indicator LEDs via the ISMS software.
 - Tamper detection shall be provided against the unit being removed from the mounting surface.
 - Keypad readers must comply with a minimum IP66 environmental protection rating.
 - Keypad readers must comply with an impact rating of at least IK08.
 - The keypad reader shall operate with a temperature range of -30°C to +70°C.

All readers must be RoHS compliant.

The keypad reader shall support a backlight feature for dark environments.

43. ACCESS CONTROL READERS – LONG RANGE

The requirement for long range access control readers will be specified in accompanying documents. When required, these readers shall meet the following specification.

The reader shall be provided in a vandal resistant enclosure, having an environmental rating of at least IP65.

The reader shall have a read range up to 10m (33ft).

The reader shall successfully read a tag/booster passing through the reader field up to 200km/hr (125mph).

Multiple channel support shall allow at least 32 readers to operate within close vicinity of each other.

A short-range access card or token shall have the ability to be temporarily associated with a booster to allow the data from the card or token to be transmitted to the long-range reader.

The transfer of data from the access card or token, through the booster, via the reader to the system shall be seamless to the end user.

A unique identifier for the booster shall be sent to the reader.

The access control decision shall be able to be based on a combination of valid access card associated with a valid booster. For example, an access decision based on a driver (cardholder ID) permitted access only with an approved vehicle (booster ID).

44. READER – BLUETOOTH AND NFC

The system shall have the capability to use a mobile device as an access credential in place of a traditional access control card.

Connectivity between the mobile device and access control reader shall be via BLE communication or NFC technology (subject to the capability of the mobile device).

In addition to BLE and NFC support, the access control reader must support multiple card and communication technologies to allow for scenarios where a mobile device may not be available. The reader shall support the following:

- Proximity 125 kHz,
- Mifare Classic,
- Mifare Plus,
- MIFARE DESFire EV1,
- MIFARE DESFire EV2.

Any communication between the ISMS and a cloud server shall be limited to those initiated by outbound requests from the ISMS only to ensure system security.

It shall be possible to configure the Bluetooth functionality of the reader via the ISMS.

The options for configuration shall include:

- enable/disable reader BLE functionality,
- enable/disable second factor authentication whereby the user must present their mobile device and enter a PIN or biometric identification,
- enable/disable the ability of the reader to advertise its name via BLE,
- adjust the overall transmit power of the reader,
- enable/disable the ability for the mobile device to automatically connect to the access control reader,
- adjust the signal strength threshold for auto connection to the access control reader,
- enable/disable the ability for the mobile device to manually connect to the access control reader,
- adjust the read range for manual connection to the access control reader.

It shall be possible to apply a global setting for all readers.

It shall be possible to apply a setting for individual readers.

It shall be possible to configure and calibrate the BLE functionality of the reader via an application on the mobile device. The configuration and calibration options shall include:

- enable/disable reader BLE functionality,
- enable/disable second factor authentication whereby the user must present their mobile device and enter a PIN or biometric identification,
- enable/disable the ability of the reader to advertise its name via BLE,
- adjust the overall transmit power of the reader,
- enable/disable the ability for the mobile device to automatically connect to the access control reader,
- adjust the signal strength threshold for auto connection to the access control reader by placing the mobile device at the distance where it is required to operate and selecting a calibration button,
- enable/disable the ability for the mobile device to manually connect to the access control reader,
- adjust the read range for manual connection to the access control reader by placing the mobile device at the distance where it is required to operate and selecting a calibration button.

Provisioning of a mobile device to be used as an access credential shall be carried out within the ISMS core software. Obtaining credential details via a third-party application or web site will not be acceptable.

Provisioning of the access credential shall be a two-step process to ensure security.

- An email shall be sent to the user who will confirm acceptance of the access credential on their mobile device.
- After acceptance, a confirmation code of no less than 6 digits shall be sent via SMS to the mobile device, whereby the user will enter this into the mobile device access control application to enable its operation.

The time allowed for the credential to be accepted shall be configurable within the ISMS. After the time has expired, the credential will need to be re-issued.

Systems that use a single step provisioning process are not acceptable. This is to avoid instances where the ISMS operator incorrectly enters an email address or mobile device number and an incorrect person receives the access credential.

It shall be possible to remove authorisation of access credentials via the ISMS should a mobile device be lost.

It shall be possible to re-issue access credentials via the ISMS should a mobile device be replaced.

It shall be possible to re-issue access credentials to another cardholder.

When the mobile device is presented to the reader, the access decision shall be made at the IFC. Systems where the access decision is made at the ISMS server or in the cloud are not acceptable.

In addition to using the mobile device as an access control credential, the following functionality shall be available via the mobile device access control application:

- arm and disarm an alarm zone,
- change the mode of a door from secure to free access, and vice versa,
- change the scheduled access mode of a door,
- activate/deactivate relay outputs anywhere on the system. The relays do not necessarily have to be connected to the access controller which is connected to the Bluetooth reader,
- receive messages from the ISMS via push notifications.

ISMS shall support Bluetooth Tag tracking utilising Bluetooth Low Energy specification outline for ibeacon and Eddystone.

45. ACCESS CONTROL READERS – BIOMETRIC (FINGERPRINT)

Where specified, biometric (fingerprint) readers are required for this project.

The reader shall be designed for wall mounting, positioned to allow ease of use for the user.

Where required, visual (LED and LCD graphic display) and audible feedback shall be provided to indicate:

- reposition the finger for a valid read,
- access granted,
- access denied.

The reader shall include a Mifare/DESFire contactless smartcard reader for verification mode where the fingerprint template is stored on a card.

The reader shall support encryption for both data in transit and data at rest for all biometric templates.

Tamper protection shall be provided against the unit being opened and against the unit being removed from the mounting surface.

The sensor resolution shall be 500dpi or greater and FBI PIV-IQS certified

Fingerprint read time shall be less than one second.

The reader shall be able to detect and reject artificial fingers presented to the reader.

46. ACCESS CONTROL READERS – BIOMETRIC (CONTACTLESS)

Where specified, contactless biometric readers are required for this project.

The reader shall be designed for wall mounting, positioned to allow ease of use for the user.

The reader shall acquire a biometric scan from a hand waved within sensor range without requiring contact to any surface.

Where required, visual (LED and LCD graphic display) and audible feedback shall be provided to indicate:

- pass hand through the sensor again for a valid read,
- access granted,
- access denied.

The reader shall include a Mifare/DESFire contactless smartcard reader for verification mode where the hand template is stored on a card.

The reader shall support encryption for both data in transit and data at rest for all biometric templates.

Tamper protection shall be provided against the unit being opened and against the unit being removed from the mounting surface.

Hand read time shall be less than one second.

The reader shall be able to detect and reject artificial hands presented to the reader.

47. ALARM MANAGEMENT TERMINAL – ACCESS CONTROL

AMTs shall be provided to allow keypad functionality as described in this section.

The AMT shall support self-discovery on the ISMS.

- AMTs shall contain a manufacturer's unique serial number.
- When connected to an IFC, the serial number of the AMT shall be reported to the ISMS.
- Once assigned to a function within an IFC, if any attempt is made to substitute AMTs in the field without authorisation, an alarm shall be generated.

Data communication rate between IFCs and AMTs shall be at least 1Mbit/second.

Communication sessions between IFCs and AMTs shall use certificate exchange protocols using keys with a minimum strength of ECC P-256.

Data communication between IFCs and AMTs shall use a minimum of AES-128.

AMTs shall generate a heartbeat signal to enable the IFC to identify lost communications and thereby generate an alarm.

AMTs shall be upgradeable via software downloaded from the ISMS without any intervention at the AMT.

Each AMT shall be identified independently on the ISMS by means of a unique plain language descriptor. The plain language descriptor shall be at least 60 characters in length.

The AMT must have a secure idle state to prevent unauthorised usage.

Where an AMT is specified, it shall include:

- The AMT must have a colour display, size being a minimum of 3.5".
- The display shall support multiple languages which shall be selectable from the ISMS software.
- The AMT shall display information to the user using a combination of text and graphics.
- The AMT shall display the date and time.

The AMT keypad shall be backlit.

The AMT keypad shall include:

- numerical 0 to 9 keys,
- a cancel key,
- an enter/accept key,
- two soft keys that vary according to the current usage of the AMT.

The AMT shall be capable of (but not limited to) carrying out the following functions:

- Arm alarm zones; a minimum of 50 per AMT must be supported.
- Disarm alarm zones; a minimum of 50 per AMT must be supported.
- View alarms; a minimum of 100 per AMT must be supported.
- Acknowledge alarms; a minimum of 100 per AMT must be supported and be decoupled from the ISMS.
- View alarm history; a minimum of 100 per AMT must be supported.
- Turn outputs on and off; a minimum of 50 per AMT must be supported.
- View the status of inputs; a minimum of 100 per AMT must be supported.
- Isolate inputs; a minimum of 100 per AMT must be supported.

User definable custom images shall be displayed on the screen when the AMT is idle.

Customisable message shall be displayed as the AMT utilised for entry and exit.

The AMT shall support the following image formats:

- PNG,
- JPG,
- JPEG.

It shall be possible to customise the AMT audio tones for Access Granted and Access Denied together with icons.

To adjust the AMT beeper via the ISMS software to the following volume levels:

- off,
- quiet,
- normal,
- loud.

Multiple AMTs can be used anywhere attached to the ISMS to remotely manage assigned intruder alarm zones.

The AMT shall have the ability to display the status of alarms and indicate the status of physical and logical items via LEDs on front panel.

The AMT shall support at least 8 indication LEDs.

It shall be possible to turn off the AMT indicator LEDs via the ISMS software.

Tamper detection shall be provided against the unit being removed from the mounting surface.

AMT readers must comply with a minimum IP66 environmental protection rating.

AMTs must comply with an impact rating of at least IK08.

The AMT shall operate within a temperature range of -30°C to +70°C.

A mobile App shall be utilised to access the AMT while using dual factor authorisation.

Cipher Pad function can be enabled to enhanced cardholder security.

48. ALARM MANAGEMENT TERMINAL – PERIMETER

AMTs shall be provided to allow keypad functionality as described in this section.

The AMT shall support self-discovery on the ISMS.

- AMTs shall contain a manufacturer's unique serial number.
- When connected to an IFC, the serial number of the AMT shall be reported to the ISMS.
- Once assigned to a function within an IFC, if any attempt is made to substitute AMTs in the field without authorisation, an alarm shall be generated.

Data communication rate between IFCs and AMTs shall be at least 1Mbit/second.

Communication sessions between IFCs and AMTs shall use certificate exchange protocols using keys with a minimum strength of ECC P-256.

Data communication between IFCs and AMTs shall use a minimum of AES-128.

AMTs shall generate a heartbeat signal to enable the IFC to identify lost communications and thereby generate an alarm.

AMTs shall be upgradeable via software downloaded from the ISMS without any intervention at the AMT.

Each AMT shall be identified independently on the ISMS by means of a unique plain language descriptor. The plain language descriptor shall be at least 60 characters in length.

The AMT must have a secure idle state to prevent unauthorised usage.

Where an AMT is specified, it shall include:

- The AMT must have a colour display, size being a minimum of 3.5".
- The display shall support multiple languages which shall be selectable from the ISMS software.
- The AMT shall display information to the user using a combination of text and graphics.
- The AMT shall display the date and time.

The AMT keypad shall be backlit.

The AMT keypad pad shall include:

- numerical 0 to 9 keys,
- a cancel key,
- an enter/accept key,
- two soft keys that vary according to the current usage of the AMT.

The AMT shall be capable of (but not limited to) carrying out the following functions:

- Arm alarm zones; a minimum of 50 per AMT must be supported.
- Disarm alarm zones; a minimum of 50 per AMT must be supported.
- View alarms; a minimum of 100 per AMT must be supported.
- Acknowledge alarms; a minimum of 100 per AMT must be supported.
- View alarm history; a minimum of 100 per AMT must be supported.
- Turn outputs on and off; a minimum of 50 per AMT must be supported.
- View the status of inputs; a minimum of 100 per AMT must be supported.
- Isolate inputs; a minimum of 100 per AMT must be supported.

Where an AMT is specified to control perimeter fence system, it shall be capable of (but not limited to) carrying out the following perimeter electric fence system functions:

- Override fence zones as follows:
 - arm,
 - disarm,
 - isolated (lock out zone(s) for maintenance).
- Display Fence Zone status ("Armed", "Disarmed", "Alarms in System") on the front panel LEDs.

-
- Display the Fence Zone status details such as High Voltage, Low Voltage and Iso-lated.
 - Display current fence return voltages.
 - Display fence return voltage range for the past seven days.
 - Display backup battery status and voltage.
 - Display current ambient temperature of the Electric Fence Controller.
 - Display the temperature range for the past seven days.

User definable custom images shall be displayed on the screen when the AMT is idle.

The AMT shall support the following image formats:

- PNG,
- JPG,
- JPEG.

It shall be possible to adjust the AMT beeper via the ISMS software to the following volume levels:

- off,
- quiet,
- normal,
- loud.

Multiple AMTs can be used anywhere attached to the ISMS to remotely manage assigned intruder alarm zones.

The AMT shall have the ability to display the status of alarms and indicate the status of physical and logical items via LEDs on front panel.

The AMT shall support at least 8 indication LEDs.

It shall be possible to turn off the AMT indicator LEDs via the ISMS software.

Tamper detection shall be provided against the unit being removed from the mounting surface.

AMT readers must comply with a minimum IP66 environmental protection rating.

AMTs must comply with an impact rating of at least IK08.

The AMT shall operate within a temperature range of -30°C to +70°C.

49. ACCESS CARDS AND TOKENS

The access token technology for this project shall match the reader technology as specified separately but in association with this specification.

Access cards shall be of standard credit card size, being no larger than CR-80 and shall be direct printable using a dye-sublimation print process or be capable of accepting an adhesive label printed through such a process.

All cards shall meet ISO standards.

As well as CR80 sized cards, vehicle tokens and key-ring transponders should also be proposed as an alternative, where available.

The access token data shall include:

- support for up to 2008-bit card numbers,
- where a proprietary card number format is offered, the card format shall include:
 - a unique site code not used for any other system worldwide,
 - a unique cardholder identification number at least 7 digits long,
 - an issue level for each card number to allow for replacing lost cards without reducing the card database size. Up to 15 levels of issue levels shall be supported.

The access control token shall uniquely identify the cardholder to the access control system.

Uniquely identifiable information shall be stored in the access token in a secure format.

Transmission of data between the proximity access token and the proximity reader shall be in a secure format.

There shall be barriers employed to prevent the copying or altering of access control data stored on the card using any readily available equipment. The tenderer shall document the barriers used.

Cards and access tokens shall be able to be encoded by the supplier according to the client's specifications, made known at the time of order.

Allowance shall be made for the supply of encoding software and hardware to the client to enable encoding of their own cards and/or tokens on site.

50. TOKEN – MIFARE CLASSIC TECHNOLOGY

The cards shall incorporate Mifare Classic technology.

The card number must be a number specifically encoded to a sector of the card. It shall not be the CSN.

The card data encoded shall use a secure sector authentication level of security to protect against card cloning. AES-128 shall be used.

The encoded card data shall incorporate data consisting of:

- the assigned card number,
- a site-specific key consisting of 32 hexadecimal characters.

Card encoding shall be an integral part of card production.

It shall be possible to specify the card sector where the card number is stored.

The Mifare sector unlock key, and the MAD unlock key shall be user definable.

Where multiple sectors on the Mifare card are configured for different applications, single pass card encoding shall be used.

51. TOKEN – MIFARE PLUS TECHNOLOGY

The cards shall incorporate Mifare Plus technology.

The card number must be a number specifically encoded to a sector of the card. It shall not be the CSN.

The card data encoded shall use a secure sector authentication level of security to protect against card cloning. AES-128 shall be used.

The Mifare Plus “S” variant shall be provided.

The encoded card data shall incorporate data consisting of:

- the assigned card number,
- a site-specific key consisting of 32 hexadecimal characters,
- the 32 hexadecimal key shall optionally be sourced from a customer specified key-safe.

Card encoding shall be an integral part of card production.

It shall be possible to specify the card sector where the card number is stored.

The Mifare sector unlock key and the MAD unlock key shall be user definable.

Where multiple sectors on the Mifare card are configured for different applications, single pass card encoding shall be used.

52. TOKEN – MIFARE DESFIRE TECHNOLOGY

The cards shall incorporate DESFire technology.

The card number must be a number specifically encoded to an application on the card. It shall not be the CSN.

The card data encoded shall use a secure sector authentication level of security to protect against card cloning. AES-128 shall be used.

The DESFire EV2 variant shall be provided.

The encoded card data shall incorporate data consisting of:

- the assigned card number.
- a site-specific key consisting of 48 hexadecimal characters.

The 48 hexadecimal key shall optionally be sourced from a customer specified key-safe

Card encoding shall be an integral part of card production.

The application unlock key and the DESFire CAD unlock key shall be user definable.

53. CREDENTIAL – BLUETOOTH AND NFC ON MOBILE DEVICE

An application shall be provided that enables a mobile device to be recognised as a valid credential for the ISMS.

The mobile device access control application shall have a built-in help system.

Credentials shall be managed with strong encryption.

It shall be possible to enable two factor authentication with the addition of either:

- PIN, or
- biometric (where supported by the mobile device).

The second authentication factor shall be selected by the user at the time of registration.

Where biometric authentication is deployed, no biometric information shall ever leave the device, this includes during the initial registration and authentication.

It shall be possible to connect the mobile device access control application to the reader for access control verification:

- Manual connection; whereby the user must interact with the mobile device access control application to request access. Interaction must be no more complex than opening the application and touching an icon relating to the reader.
- Auto-connection; whereby the phone is authorised with a reader when the signal strength reaches a configured threshold, and does not have to open the application and touch an icon.

Provisioning of the access credential shall be a two-step process to ensure security. After acceptance, a confirmation code of no less than 6 digits shall be sent to the mobile device,

whereby the user will enter this into the mobile device access control application to enable its operation.

The mobile device access control application shall support multiple sites without requiring the device holder to change any settings to move between sites.

The mobile device access control application shall support a digital ID:

- Displaying all the information as is available in the integrated card design program.
- The digital ID shall display the time that the information was verified on the ISMS server.
- If the digital ID is not able to verify with the ISMS server, then this shall be displayed as an additional message overlaying the digital ID.

54. CREDENTIAL - BIOMETRIC

The requirement for biometric authentication will be specified in accompanying documents. When required the following specifications shall be met.

The biometric readers and associated technology shall be fully integrated into the system. All biometric enrolment and template management user interfaces shall be provided seamlessly in the standard central control system user interface.

The operator shall not have to access a separate biometric template database to manage biometric templates.

The identification time (time to identify a presented biometric from the database) shall be less than 2 seconds.

The reader shall have tamper protection against removal of the reader from the wall, and removal of the reader fascia from the base.

Enrolment shall be carried out at a USB capable enrolment reader specifically provided for this purpose.

The enrolled biometric templates shall conform to the following:

- Each template shall be based on three separate presentations to obtain the best template.
- A second template associated with a second biometric (in case the primary biometric temporarily cannot be used for any reason) shall be enrolled.
- Two optional duress biometric templates shall be able to be captured and stored in the reader.
- The enrolment user interface shall provide visual and audible guidance for correct biometric presentation during enrolment.
- The enrolment user interface shall display a quality score associated with the biometric capture and warn the operator if the quality of the template is low.

-
- The enrolment user interface shall provide an indication of the enrolment quality of the presented biometrics. The level of quality threshold for accepting presented biometrics shall be adjustable by the operator.

When identification mode (1 to many, or 1:N) is specified:

- The enrolment reader shall read the biometrics and store them as biometric templates in a central database.
- The biometric templates defined above shall be a subset of the cardholder record.
- During the biometric read process, the presentation of a biometric at a reader shall initiate a database inquiry at the reader. If the biometric is determined to be of a valid cardholder, the associated access will then be verified by the access controller before access is granted.

When verification mode 1 to one, or 1:1 is specified:

- The enrolment reader shall read the biometrics and store the template data onto a Mifare Classic, Mifare Plus, or DESFire card.
- When the card is to be encoded, the user shall be prompted to enrol the biometrics and the card shall then be encoded with both the system identification data and the biometric data.
- There shall be a configurable option whether to save cardholder biometrics to the central database or discard after encoding to card.
- During the biometric read process, the biometric read at a reader shall be compared with the template data read from the card. If the biometric is determined to be a match, then the associated access will be verified by the access controller before access is granted.
- An authorised system operator shall be able to generate and download a Mifare A key to all readers in the system.
- The A key shall be either generated automatically as a random hexadecimal key, or manually entered.
- On a Mifare Classic or Mifare Plus card, the Mifare sectors where the biometric template data is to be stored shall be user definable.

55. RS485 FIBRE TRANSCEIVER REQUIREMENTS

The fibre transceiver shall provide two independent data channels operating as either multi-mode or single-mode devices (depending on the model).

Each channel will be capable of transparently supporting data speeds of 1MB/S on a single fibre.

Each data channel will be capable of handling 2-wire half-duplex RS485 data as per the TIA/EIA standards.

The multi-mode fibre transceiver shall be capable of supporting distances up to 4km between fibre transceivers.

The single-mode fibre transceiver shall be capable of supporting distances up to 40km between fibre transceivers.

Up to 60 devices per RS485 channel shall be supported.

The fibre transceiver shall support the following network topologies:

- point-to-point,
- multi-drop,
- redundant self-healing ring topology.

The fibre transceiver will provide indication of port faults and network damage which shall support the following:

- LED indication at the unit,
- relay output at the unit,
- configurable to indicate either local or global (all transceivers) faults.

LED indicators on the fibre transceiver shall indicate the following:

- data activity,
- synchronisation status,
- fault status,
- fault location.

Each channel shall support individually selectable RS485 biasing via a dip-switch.

The operating temperature for the fibre transceiver will be -40°C to +75°C.

The fibre transceiver shall have reverse polarity protection.

Mean time between failure for the fibre transceiver should be no less than 100,000 hours.

56. ENERGISED PERIMETER INTRUDER DETECTION - STRUCTURE

The physical fence part of the energised intruder detection system shall be a multi-wire Energised Security Fence (ESF) which consists of a horizontally spaced grid of conductive wires supported by a specially made carrier fence. This will comprise of insulated components exclusively used for a security fence, and support posts retro-fitted to an existing solid and/or mesh type fence or wall.

The system shall be installed in accordance with the manufacturer's installation instructions.

The operating voltage for the energised fence shall be a high voltage short duration pulse, managed and continually monitored to deter intrusion by giving any intruder a high voltage pulse should they touch any part of the grid of conductive wires whilst earthed or in contact with other conductive elements.

All energised fence wires must deliver a deterrent pulse to an intruder touching a wire and earth, or attempting to penetrate between any adjacent wires.

The ESF shall contain intermediate insulating posts at a spacing not greater than three metres to minimise ability to spread the grid of conductive wires creating a viable opening in the energised fence.

Physical hardware (e.g. tensioning devices, springs and insulators) should be inherently designed to suit security applications. Items designed and used for agricultural applications will not be acceptable.

Intermediate insulating components shall have a minimum electrical tracking distance of not less than 80mm.

Intermediate insulating components shall have no area where the conductive wires can be trapped easily between insulator surfaces of the insulating components if the conductive wire is demounted from its nominal position on the insulating component.

Shielding of insulating components should be designed to direct the conductive wire to an earth contact to maximise alarm generation if the conductive wire is demounted from its nominal position.

The retention mechanism of the conductive wire on the insulating components shall be designed to break during climbing attempts where a load greater than 30kg is applied in a direction away from the physical fence structure.

All structural climb points must be fitted with additional intrusion detection and anti-climb protection.

The conductive wires shall be attached to the inner face of the barrier security fence and access gates when installed within 1.5m of ground level. The barrier security fence provides a physical separation barrier between the general public and the exposed pulsed conductive wires.

Unless otherwise specified, the conductive wires shall extend at least 0.6 metres above the top of the existing barrier security fence fabric or a minimum of 1.0 metre above a wall.

Each energised fence circuit on the same fence control device must be capable of being operated independently.

Where two fence circuits are operating within the same detection zone, shorting of one conductive wire to earth or another conductive element (excluding second conductive wire) should not directly affect the performance and detection of the second conductive wire.

Each access gate or perimeter access door shall be fitted with a switching device that will detect the opening of the gate/door. The switching device and/or attached controls shall ensure all high voltage pulses on or around the gate/door are effectively shorted to earth or disabled at the fence controller.

Opening of a perimeter access door or gate should annunciate an alarm condition on the system and inhibit the deterrent pulses on that gate.

Each active fence circuit shall be individually configurable for all functionalities.

Anti-climb configuration at strain points shall be provided, above the physical barrier. The fence circuit shall be routed around strain posts and connected to strainers such that it forms part of the continuous electrical circuit and does not constitute a parallel, redundant or dead-end path.

Re-tensioning of fence wires must be possible without the need to reposition anti-climb elements.

All joints between conductive elements in a fence circuit shall be clamped and not rely solely on tension of the conductive wire to maintain the integrity of the electrical connection. This excludes the external pressure contact between gate switch halves.

All metal components of the system must be protected against the environment using aluminium alloy, or steel with zinc-based galvanising.

- Copper based components are not permitted.
- Stainless steel should not be mechanically or electrically coupled to aluminium or zinc galvanised components without measures to prevent galvanic corrosion.

Security posts shall be galvanised to ensure maximum environmental protection and performance.

The termination point of the conductive wire should be at the tensioning device.

Tensioning devices should be attached to the ESF structure by insulated mounting hardware. Tensioners that are attached to the ESF structure by wire hooks shall not be acceptable.

Fine pitch tensioning capability shall be provided for ease of adjustment during installation and maintenance.

The tensioning of the conductive wire shall be integrated into the tensioning device directly attached to the security fence post. Independent tensioning devices shall not be acceptable.

Re-tensioning of conductive wire must be possible without the need to reposition the configuring links.

Where springs are attached to the grid of conductive wires, an indication of the tension of the conductive wire must be clearly visible on the spring device.

Where springs are attached to the grid of conductive wires, the spring must be in direct electrical contact to the tensioning device.

Springs used in the tensioning of the conductive wire should be of a single continuous wire which forms part of the conductive circuit.

Any spring which form part of the conductive circuit should have a means of physically limiting the length of extension of the spring.

Each conductive wire shall be capable of deterring and detecting potential intruders by means of a high voltage pulse and detecting the following types of attack:

- cutting or disconnecting any wire,
- shorting any wire to ground or the support fence,
- shorting adjacent but different polarity wires,
- shunting the wires with an electrically conductive material to reduce the pulse voltage.

Each active fence circuit shall always be monitored.

The system shall be configured in accordance with the specific contract drawings.

The system shall generate an alarm within four seconds if any one wire is cut or continuously short circuited to an adjacent wire or to earth.

The shorting together of any conductive wires, or cutting of any wires, shall have no impact on the deterrent or detection capability of the remaining active fence circuits and zones.

The shorting together of any conductive wires, or cutting of any wires, shall raise an alarm in the ISMS.

The system shall generate minimal nuisance alarms in any environmental conditions of wind, rain, or temperature, nor from wildlife of less than five kilograms.

The system shall have a false alarm rate no greater than one false alarm per fence line kilometre per week.

All fence pulses shall be synchronised so that the pulses on adjacent fence sections do not occur at a time interval less than permitted in the current version of relevant standards (IEC60335-2-76).

When specified, local control at field cabinets shall be provided via an AMT.

Fully adjustable lightning diverter and protection devices shall be connected to each ESF circuit connection.

An independent earthing system must be provided for the ESF earth return with a physical separation of 10m from any other earthing system.

Where the ESF abuts to, attaches to or passes over any metallic structure, that structure must be grounded or earthed using a separate earthing system.

When specified, the ESF must be capable of interfacing with an emergency shutdown system, which in the event of an incident will electronically deactivate and isolate the high voltage deterrent pulses on the conductive wire array.

- The emergency shutdown when specified shall be a fail-safe interface, carried out at each of the field cabinets to minimise dependency on site communication systems.

The system manufacturer shall support the product for a minimum period of ten years from the time at which the product is superseded.

The system must be formally inspected and assessed by a manufacturer approved representative, to the manufacturer's published standard.

Full system documentation meeting the manufacturer's compliance, minimum quality, safety codes, and instruction must be provided to the system end user representative.

An annual preventative maintenance program must be offered to check and maintain the ESF to an operational and safe condition.

57. ENERGISED SECURITY FENCE CONTROLLER – STAND ALONE

The physical fence part of the energised intruder detection system shall be a multi-wire ESF which consists of a horizontally spaced grid of conductive wires supported by a specially made carrier fence. This will comprise of insulated components exclusively used for a security fence, and support posts retro-fitted to an existing solid and/or mesh type fence or wall.

The ESF controller shall generate pulses at intervals of not less than 1.1 seconds.

The ESF controller shall be available as a single fence circuit or dual fence circuit option.

The ESF controller shall be capable of delivering 2.3 Joules when configured as a live/earth system, i.e. alternate wires have a voltage or are earthed.

The ESF controller shall be capable of delivering 4.6 Joules when configured as a dual-pulse system, i.e. alternate conductive wires have positive to negative voltages.

The ESF controller shall provide an optional reduced voltage operating mode to provide full detection capability as per high voltage but with reduced deterrent.

An alternative ESF controller shall be available with the following capabilities where the project requires:

- When configured as a live/earth system, the ESF Controller shall be capable of increasing the output from 2.3 Joules to 3.6 Joules per fence circuit. This is triggered when there is a drop in voltage from one high voltage pulse to the next, which has reached a pre-defined alarm threshold.
- When configured as a dual-pulse system, the ESF Controller shall be capable of increasing the output from 4.6 Joules to 7.2 Joules. This is triggered when there is a drop in voltage from one high voltage pulse to the next, which has reached a pre-defined alarm threshold. Output is measured across alternate wires.
- The ESF shall return to the standard output after 20 minutes.

The conductive wire pulses shall be synchronised so that the pulses on adjacent fence sections occur within time intervals as permitted in the reference standards.

The ESF controller shall operate within an ambient temperature range of -20°C to +50°C.

The ESF controller shall have temperature sensors to monitor the internal temperature of its enclosure and adjust performance as follows:

- 75°C. Over-temperature.
 - An indicator LED on the front panel shall flash and the ESF controller shall reduce its pulse rate to reduce the internal temperature
- 85°C Critical temperature.
 - The ESF controller must stop generating pulses and turn off.

The ESF controller shall have indicator LEDs on the front panel to indicate the following:

- over temperature alarm,
- service alarm,
- tamper,
- mains power failure,
- battery test failed, or battery missing,
- high voltage mode,
- low voltage mode,
- fence circuit pulsing with return voltage measurement in the form of a bar-LED indicator,
- synchronisation status:
 - off,
 - synchronisation conflict,
 - correct synchronisation.

The ESF controller shall have a service mode to allow a service technician to easily isolate and locally control fence circuits.

This service mode shall be accessible at the ESF controller by means of a special key.

The ESF controller shall provide battery management as follows:

- trickle charge; slow charge rate when battery is below 10 VDC,
- bulk charge; maximum charge rate for fast battery recovery,
- float charge; slow charge rate to accommodate temperature variations,
- battery save; reduce electric pulse rate to save battery power.

The ESF controller shall support external power supplies such as additional backup batteries or solar cells to be connected.

The ESF controller shall operate in a standalone mode such that it does not require any external system software for its configuration and control.

Configuration shall be via dip-switches inside the ESF controller.

The fence circuits shall be armed and disarmed via input signals from an external switch, keypad, or alarm panel.

The ESF controller shall have output relays to indicate the following:

- system alarm,
- power supply failure,
- primary fence circuit alarm,
- armed status,
- secondary fence circuit alarm, for the dual fence circuit ESF controller.

The ESF controller shall have the capability to be changed from a standalone unit to a networked unit which is connected to an ISMS via a dip-switch, without the need to change any firmware within the ESF controller.

58. ENERGISED SECURITY FENCE CONTROLLER - NETWORKED

The ESF controller shall deliver an electric pulse through the fence wires to maximise the intruder deterrent and detection capabilities whilst meeting global safety standards.

The ESF controller shall operate in a networked environment and be controlled and monitored by the ISMS.

The ESF controller shall generate pulses at intervals of not less than 1.1 seconds.

The ESF controller shall be available as a single fence circuit (single zone) or dual fence circuit (dual zone) option.

The ESF controller shall be capable of delivering 2.3 Joules when configured as a “live/earth” system, i.e. alternate wires have a voltage or are earthed.

The ESF controller shall be capable of delivering 4.6 Joules when configured as a dual-pulse system, i.e. alternate conductive wires have positive to negative voltages.

The ESF controller shall provide an optional reduced voltage operating mode to provide full detection capability as per high voltage but with reduced deterrent.

The ESF controller shall support self-calibrating alarm thresholds that vary the required voltage drop to generate an alarm in response to long-term environmental factors.

An alternative ESF controller shall be available with the following capabilities where the project requires:

- When configured as a live/earth system, the ESF Controller shall be capable of increasing the output from 2.3 Joules to 3.6 Joules per fence circuit. This is triggered when there is a drop in voltage from one high voltage pulse to the next, which has reached a pre-defined alarm threshold.
- When configured as a dual-pulse system, the ESF controller shall be capable of increasing the output from 4.6 Joules to 7.2 Joules. This is triggered when there is a drop in voltage from one high voltage pulse to the next, which has reached a pre-defined alarm threshold. Output is measured across alternate wires.
- The ESF shall return to the standard output after 20 minutes.

The conductive wire pulses shall be synchronised so that the pulses on adjacent fence sections occur within time intervals as permitted in the reference standards.

The ESF controller shall operate within an ambient temperature range of -20°C to +50°C.

The ESF controller shall have temperature sensors to monitor the internal temperature of its enclosure and adjust performance as follows:

- 60°C Temperature warning.
 - It shall be possible to activate a relay to turn on an external cooling fan.
- 75°C Over-temperature.
 - An indicator LED on the front panel shall flash and the ESF controller shall reduce its pulse rate to reduce the internal temperature
- 85°C Critical temperature.
 - The ESF controller must stop generating pulses and turn off.

The ESF controller shall have indicator LEDs on the front panel to indicate the following:

- over temperature alarm,
- service alarm,
- tamper,
- mains power failure,
- battery test failed, or battery missing,
- high voltage mode,
- low voltage mode,
- fence circuit pulsing with return voltage measurement in the form of a bar-LED indicator,
- synchronisation status:
 - off,

-
- synchronisation conflict,
 - correct synchronisation.

The ESF controller shall have a service mode to allow a service technician to isolate and locally control fence circuits.

- An event shall be sent to the system when the ESF controller is in service mode.
- The service mode shall be capable of being enabled from the ISMS.
- This service mode shall be toggled at the ESF controller by means of a special key when enabled by the ISMS.

The ESF controller shall provide battery management as follows:

- trickle charge; slow charge rate when battery is below 10 VDC,
- bulk charge; maximum charge rate for fast battery recovery,
- float charge; slow charge rate to accommodate temperature variations,
- battery save; reduce electric pulse rate to save battery power.

The ESF controller shall support external power supplies such as additional backup batteries or solar cells to be connected.

The ESF controller shall support self-discovery on the ISMS.

- ESF controller shall contain a manufacturer's unique serial number.
- When connected to an IFC, the serial number of the ESF controller shall be reported to the ISMS.
- Once assigned to a function within an IFC, if any attempt is made to substitute ESF controllers in the field without authorisation, an alarm shall be generated.

Data communication rate between IFC and the ESF controller shall be at least 1Mbit/second.

Communication sessions between IFC and ESF controller shall use certificate exchange protocols using keys with a minimum strength of ECC P-256.

Data communication between IFCs and ESF controllers shall use a minimum of AES-128.

ESF controllers shall generate a heartbeat signal to enable the IFC to identify lost communications and thereby generate an alarm.

ESF controllers shall be upgradeable via software downloaded from the ISMS without any intervention at the controller.

59. SYSTEM INTEGRATION

The ISMS shall support OPC AE protocol.

-
- The OPC AE interface shall allow third party OPC clients to subscribe to receive alarms and events from the ISMS.
 - When an alarm is processed, the OPC AE client shall send an event processed message back to the ISMS to process the alarm on the ISMS.
 - The ISMS shall support multiple simultaneous OPC AE connections.

The ISMS shall support OPC DA protocol.

- The OPC interface shall support OPC DA specification 2.0 and 3.0.
- The OPC DA interface shall allow the status of system components to be reported to an external OPC DA client.
- The OPC Interface shall allow third party OPC DA clients to generate system component overrides including but not limited to alarm zone and access zone overrides.
- The ISMS shall support multiple simultaneous OPC DA connections.

The ISMS shall support a REST Web Service API.

- The ISMS cardholder functionality shall support a REST Web Service to allow an external system to create, remove, and modify cardholders, including assigning access rights.
- The ISMS alarms and events functionality shall support a REST Web Service to allow external systems to receive alarms and events from the ISMS.
- The ISMS shall provide a REST Web Service that will allow a third-party system to perform actions in the ISMS such as open doors, disarm alarm zones, and turn an IFC output on.
- The ISMS shall support a REST Web Service that will allow a third-party system to interrogate the status of ISMS items such as doors, alarm zones, and IFC inputs.

The ISMS shall allow data exchange with other applications using XML protocols.

- The system shall provide an XML interface to allow for the import, export, and synchronisation of data in an on-going basis from other applications directly into the cardholder database both in a real-time manner and in a batch-oriented approach. A developer's kit with a sample application shall be readily available.
- The system shall provide an XML interface to allow for updating access control schedules from other applications directly into the ISMS database in both a real-time manner and in a batch-oriented approach. A developer's kit with sample application shall be readily available.

The system shall provide a tool which allows configuration and synchronisation of cardholder data with third party systems via a csv file. The CSV import functionality shall support the following functionality:

- manually triggered data import,

-
- schedule triggered data import,
 - images imported via flat file.

An API that communicates directly to the IFC shall be available.

- The API shall allow third party systems to pass events to the IFC and for the events to appear in the ISMS event window.
- It shall be possible for the IFC to be programmed to trigger actions based upon these external events. For example, a video analytic alarm from a video management system is passed to the IFC, the IFC in turn will lock doors and raise an alarm.
- It shall be possible for a third-party system to send a card number and site code to the IFC to act as a “virtual card reader”.
- The API shall allow the third-party system to interact directly with the IFC with no reliance on the ISMS server.

The ISMS shall support the BACnet communications protocol.

- BACnet communication will be via TCP/IP.
- The IFC will communicate with BACnet devices with no need for server intervention.
- The BACnet integration will enable the IFC to monitor BACnet objects for state changes and raise alarms accordingly.
- The BACnet integration will enable the IFC to change BACnet object states in response to events.

The ISMS shall support the SNMP communications protocol.

Events from third party systems shall be managed in the same way as inputs connected directly to IFCs.

Interactions with third party systems shall be logged in the ISMS.

ISMS shall support smart sensor integration which detects the following

- Masking
- Air quality
- Volatile organics
- Vaping
- Gunshot
- Tetrahydrocannabinol (THC)
- Fine particulate matter (PM 2.5 and PM10)

-
- Ammonia
 - Nitrogen dioxide
 - Carbon monoxide
 - Carbon dioxide
 - Help keyword
 - Aggression
 - Barometric pressure
 - Light level
 - Temperature
 - Humidity
 - Tampered
 - Sound level

The system shall support biometric reader integration which can read all four fingerprints on a cardholder's hand.

The ISMS shall have the ability to integrate with SIP intercoms and provide the following functionality

- Answer calls from the ISMS
- Call a SIP intercom from ISMS
- Please a call on hold
- Hanging up a call
- View video for an intercom at 720p resolution
- Grant access

60. VIDEO MANAGEMENT SYSTEM INTEGRATION

The ISMS shall be capable of concurrently interfacing with VMS from multiple vendors.

It shall be possible for the ISMS to view live video from multiple cameras within its interface.

The ISMS shall be capable of viewing stored (archived) video from the VMS within its interface.

Where supported by the integrated VMS, it shall be possible to operate camera controls such as:

- PTZ,

-
- pause,
 - forward,
 - rewind.

It shall be possible to maximise a camera window.

- Whilst a camera window is maximised, the other camera windows should be changed to live thumbnail images to ensure the operator is able to see activity in all cameras.

It shall be possible to drag a camera icon from a site plan into a video view to dynamically be able to view cameras in an ad hoc manner.

It shall be possible to drag a camera icon from a list into a video view to dynamically be able to view cameras in an ad hoc manner.

It shall be possible to find a camera from a search box.

Where supported by the integrated VMS, it shall be possible for the ISMS to send a message to the VMS to move cameras to priests.

Where supported by the integrated VMS, it shall be possible for the ISMS to receive motion detection and video analytic events from the VMS.

61. REST API

The ISMS shall support a RESTful web API.

The RESTFUL API shall support client certificate pinning for connection security.

The RESTful API shall be authenticated and secured using TLS client certificates (2048-bit RSA).

The RESTFUL API shall support HTTPS for data transfer.

Rest API should allow Cardholder data Synchronisation between ISMS servers

Rest API shall be able to interface to the Visitor Management setup on the ISMS in order to set up the following

- Create Visitor
- Modify any Visit attributes
- Delete Visitor

ISMS shall allow Restful APIs to create, amend and delete access schedules as a requirement for a single source of truth.

Restful API shall allow for mixed key-and-certificate authentication

Restful APIs are utilised for Active Directory Cardholder Synchronisation

The system shall support Events and Cardholder data Synchronisation from a source to destination servers by utilising Rest APIs.

The web-based client shall use REST API via an API Gateway that has no persistent storage.

The ISMS shall send updates to web-based client session through use of Rest APIs via API Gateway.

REST API shall allow the users to redact Personal Identifiable Information (PII) from the system in order to meet GDPR requirements

PART C4: SITE INFORMATION

C4: SITE INFORMATION

C4.1 SITE INFORMATION

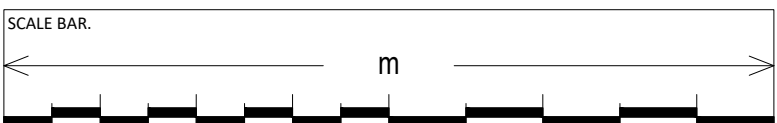
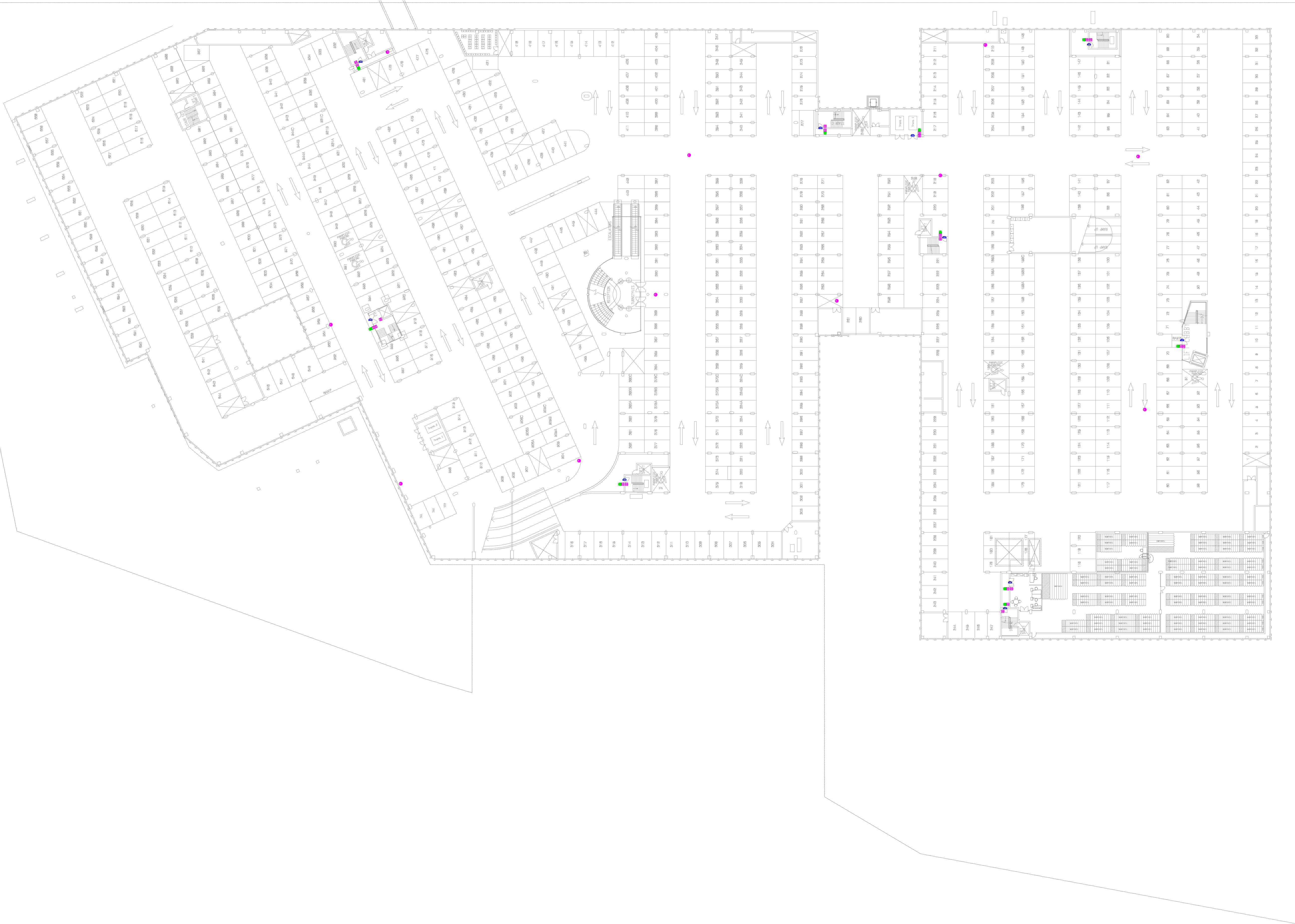
The site is located on 77 Meintjies Street, Trevenna, Sunnyside Pretoria. Tenderers are to familiarise themselves with the site to determine routes for site access, restrictions and proximity to existing structures.

The site GPS coordinate are as follows: -25.75021; 28.20004

Latitude: 25.75021"S / 25° 45' 01.04" S
Longitude: 28.20004"E / 28° 12' 00.14" E

Figure 1 – Aerial View of the dtic campus showing block arrangement





LEGEND			
Symbol	QTY	Description	
	21	PROXIMITY CARD READER.	
	10	SECURITY BREAK GLASS UNIT (Green).	
	10	MAGNETIC LOCK.	
	11	DOME CCTV CAMERA.	

FOR TENDER

REV.

DATE.

DESCRIPTION.

BY.

PROJECT:

DTIC CAMPUS

DETAILS:

LOWER BASEMENT PARKING
ACCESS CONTROL & CCTV LAYOUT

DRAWN.

AT

CHECKED.

INCEPTION DATE.

2025.08.13

SCALE.

A1: 1:125

DRAWING NO.

DTI/BAS/ONE/SEC/01

REV.

A

PROJECT MANAGER
NAME:
NUMBER:
EMAIL:

ACCOUNT MANAGER
NAME:
NUMBER:
EMAIL:

MEINTJES STREET

TREVENA

LEGEND			
Symbol	QTY	Description	
	48	PROXIMITY CARD READER.	
	19	SECURITY BREAK GLASS UNIT (Green).	
	19	MAGNETIC LOCK.	
	51	DOME CCTV CAMERA.	
	1	NETWORK SWITCH.	

FOR TENDER

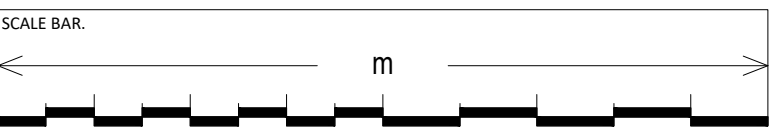
REV.	DATE.	DESCRIPTION.	BY.
------	-------	--------------	-----



DTIC CAMPUS

DETAILS:			
UPPER BASEMENT ACCESS CONTROL & CCTV LAYOUT			
DRAWN. AT	CHECKED.	INCEPTION DATE. 2025.08.13	SCALE. A1: 1:125
DRAWING NO. DTI/BAS/TWO/SEC/01			REV. A

PROJECT MANAGER NAME: NUMBER: EMAIL:	ACCOUNT MANAGER NAME: NUMBER: EMAIL:
---	---





Symbol		QTY	LEGEND	Description
		21	PROXIMITY CARD READER.	
		11	SECURITY BREAK GLASS UNIT (Green).	
		11	MAGNETIC LOCK.	
		10	DOME CCTV CAMERA.	
		9	NEW CCTV CAMERA.	
			No color scheme assign	

FOR TENDER

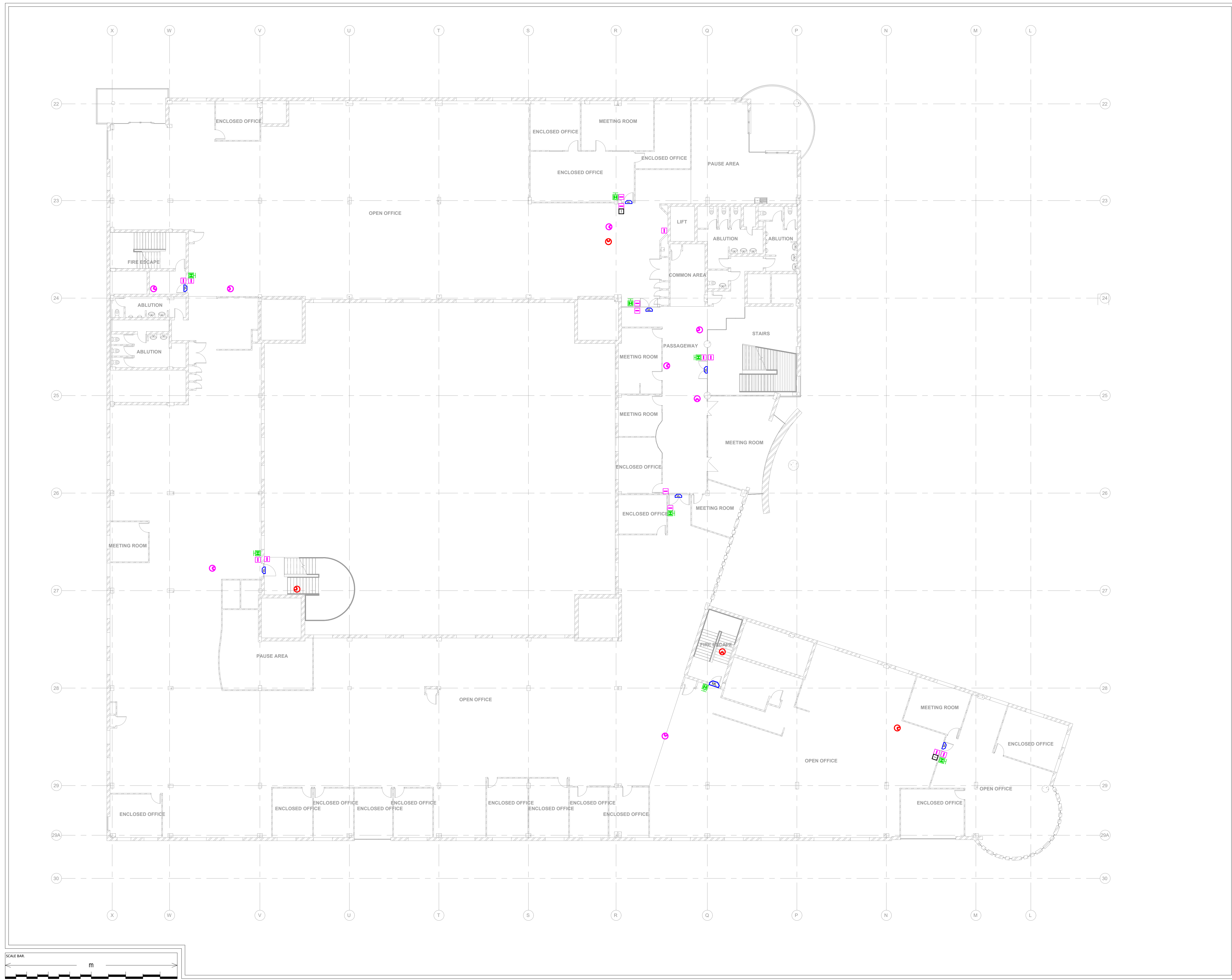
REV.	DATE.	DESCRIPTION.	BY.

PROJECT:
DTIC CAMPUS

DETAILS:
**BLOCK A - FIRST FLOOR
ACCESS CONTROL & CCTV LAYOUT**

DRAWN: CP	CHECKED:	INCEPTION DATE: 2025.08.13	SCALE: A1: 1:125
DRAWING NO. DTI/A/1ST/SEC/01			REV. A

PROJECT MANAGER NAME: NUMBER: EMAIL:	ACCOUNT MANAGER NAME: NUMBER: EMAIL:
---	---



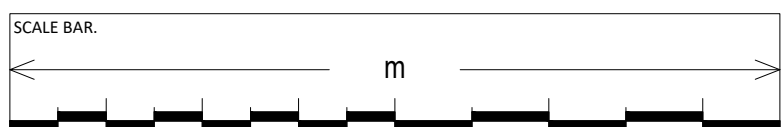
LEGEND		
Symbol	QTY	Description
	15	PROXIMITY CARD READER.
	8	SECURITY BREAK GLASS UNIT (Green).
	8	MAGNETIC LOCK.
	8	DOME CCTV CAMERA.
	4	NEW CCTV CAMERA.
	2	INTERCOM

FOR TENDER

REV.	DATE.	DESCRIPTION.	BY.
------	-------	--------------	-----



PROJECT:			
DTIC CAMPUS			
DETAILS:			
BLOCK A - SECOND FLOOR ACCESS CONTROL & CCTV LAYOUT			
DRAWN:	CHECKED:	INCEPTION DATE:	SCALE:
		2025.08.13	A1: 1:125
DRAWING NO.	DTI/A/2ND/SEC/01		REV.
			A
PROJECT MANAGER NAME: NUMBER: EMAIL:		ACCOUNT MANAGER NAME: NUMBER: EMAIL:	



LEGEND		
Symbol	QTY	Description
	49	PROXIMITY CARD READER.
	24	SECURITY BREAK GLASS UNIT (Green).
	24	MAGNETIC LOCK.
	7	DOME CCTV CAMERA.
	1	NETWORK SWITCH.

FOR TENDER

REV.	DATE.	DESCRIPTION.	BY.
------	-------	--------------	-----



PROJECT:			
DTIC CAMPUS			
DETAILS:			
BLOCK A - THIRD FLOOR ACCESS CONTROL & CCTV LAYOUT			
DRAWN: AT	CHECKED:	INCEPTION DATE: 2025.08.13	SCALE: A1: 1:125
DRAWING NO. DTI/A/3RD/SEC/01			REV. A

PROJECT MANAGER NAME: NUMBER: EMAIL:	ACCOUNT MANAGER NAME: NUMBER: EMAIL:
---	---



LEGEND		
Symbol	QTY	Description
	19	PROXIMITY CARD READER.
	6	SECURITY BREAK GLASS UNIT (Green).
	6	MAGNETIC LOCK.
	11	DOMESTIC CCTV CAMERA.
	6	NEW CCTV CAMERA.
	1	CCTV CAMERA.
	1	CCTV CAMERA WITH PAN, TILT & ZOOM.

FOR TENDER

REV.	DATE.	DESCRIPTION.	BY.

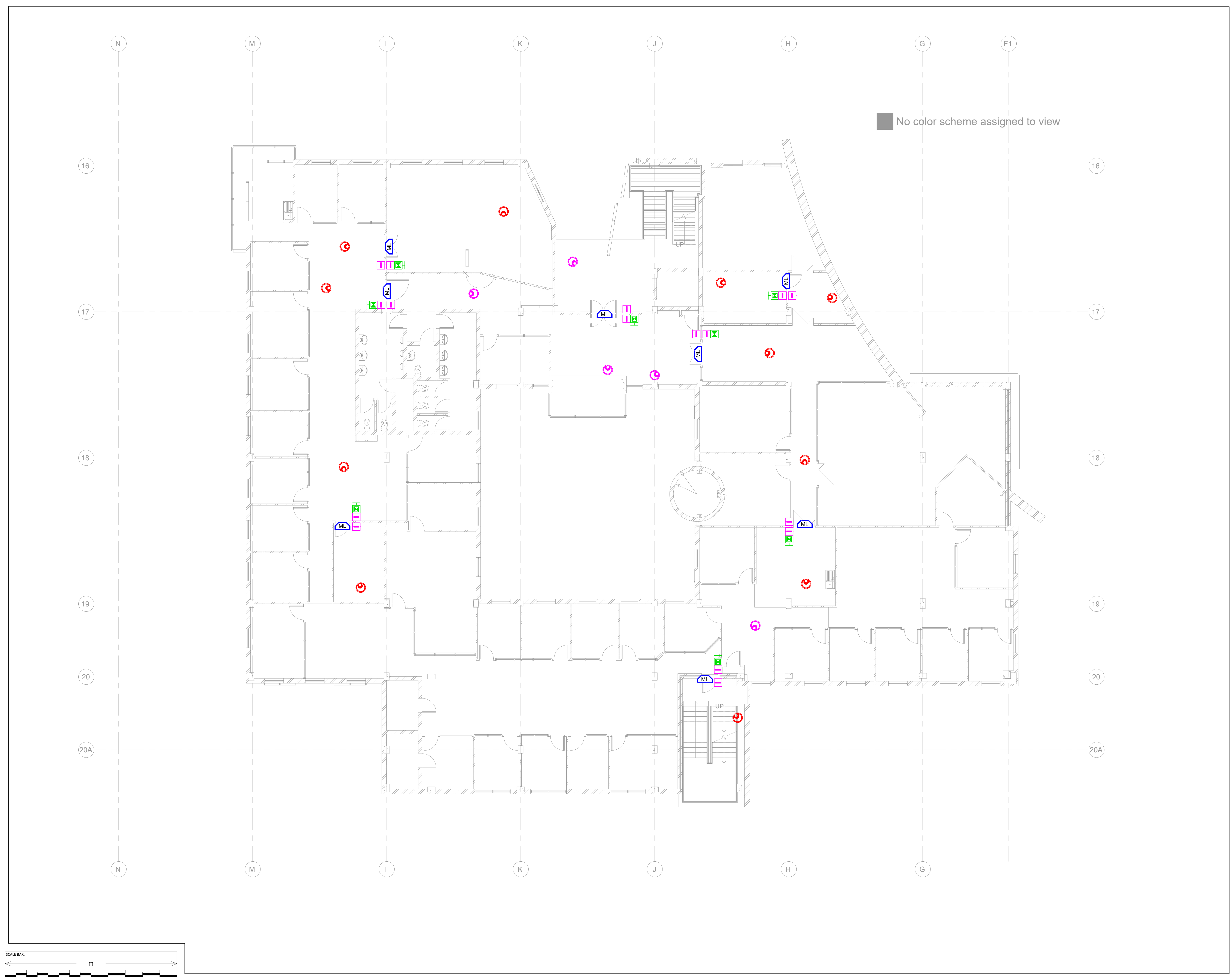
PROJECT:
DTIC CAMPUS

DETAILS:
**BLOCK A - GROUND FLOOR
ACCESS CONTROL & CCTV LAYOUT**

DRAWN.	CHECKED.	INCEPTION DATE.	SCALE.
CP		2025.08.13	A1: 1:125

DRAWING NO.	REV.
DTI/A/GND/SEC/01	A

PROJECT MANAGER	ACCOUNT MANAGER
NAME:	NAME:
NUMBER:	NUMBER:
EMAIL:	EMAIL:



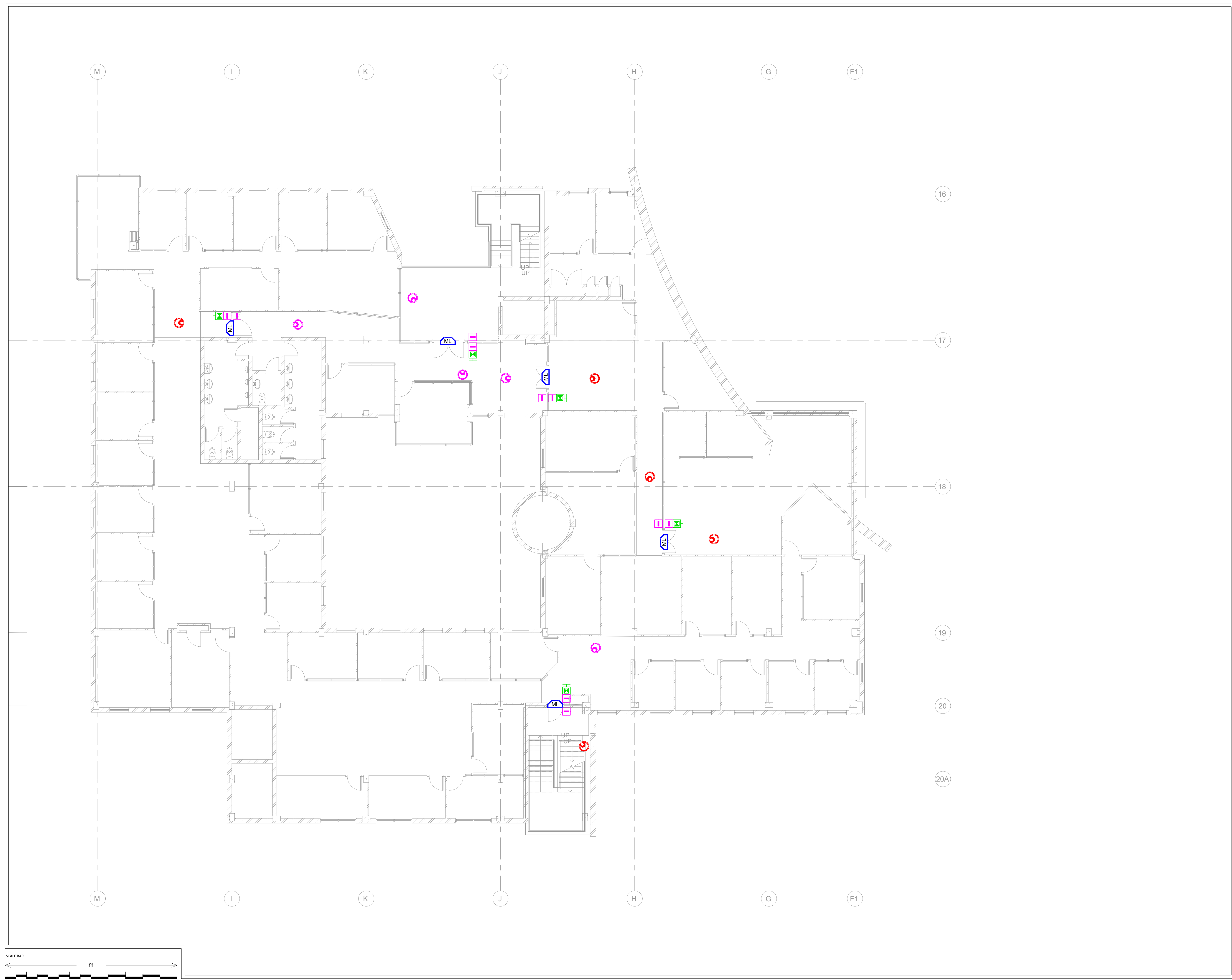
LEGEND		
Symbol	QTY	Description
	16	PROXIMITY CARD READER.
	8	SECURITY BREAK GLASS UNIT (Green).
	8	MAGNETIC LOCK.
	5	DOME CCTV CAMERA.
	11	NEW CCTV CAMERA.

FOR TENDER

REV.	DATE.	DESCRIPTION.	BY.
------	-------	--------------	-----



PROJECT:			
DTIC CAMPUS			
DETAILS:			
BLOCK C - FIRST FLOOR ACCESS CONTROL & CCTV LAYOUT			
DRAWN:	CHECKED:	INCEPTION DATE:	SCALE:
		2025.08.13	A1: 1:125
DRAWING NO.			REV.
DTI/C/1ST/SEC/01			A
PROJECT MANAGER NAME: NUMBER: EMAIL:		ACCOUNT MANAGER NAME: NUMBER: EMAIL:	



LEGEND		
Symbol	QTY	Description
	10	PROXIMITY CARD READER.
	5	SECURITY BREAK GLASS UNIT (Green).
	5	MAGNETIC LOCK.
	5	DOME CCTV CAMERA.
	5	NEW CCTV CAMERA.

FOR TENDER

REV.	DATE.	DESCRIPTION.	BY.
------	-------	--------------	-----



PROJECT:			
DTIC CAMPUS			
DETAILS:			
BLOCK C - SECOND FLOOR ACCESS CONTROL & CCTV LAYOUT			
DRAWN:	CHECKED:	INCEPTION DATE:	SCALE:
		2025.08.13	A1: 1:125
DRAWING NO.	DTI/C/2ND/SEC/01		REV.
			A
PROJECT MANAGER NAME: NUMBER: EMAIL:		ACCOUNT MANAGER NAME: NUMBER: EMAIL:	



LEGEND		
Symbol	QTY	Description
	14	PROXIMITY CARD READER.
	7	SECURITY BREAK GLASS UNIT (Green).
	7	MAGNETIC LOCK.
	5	DOME CCTV CAMERA.
	9	NEW CCTV CAMERA.

FOR TENDER

REV.	DATE.	DESCRIPTION.	BY.
------	-------	--------------	-----



PROJECT:		DTIC CAMPUS	
DETAILS:		BLOCK C - THIRD FLOOR ACCESS CONTROL & CCTV LAYOUT	
DRAWN:	CHECKED:	INCEPTION DATE: 2025.08.13	SCALE: A1: 1:125
DRAWING NO. DTI/C/3RD/SEC/01		REV. A	
PROJECT MANAGER NAME: NUMBER: EMAIL:		ACCOUNT MANAGER NAME: NUMBER: EMAIL:	



NOTE:

- REVIT DRAWING LAYOUT PROVIDED DIFFERS FROM MARKUP PDF LAYOUT PROVIDED.

LEGEND		
Symbol	QTY	Description
	18	PROXIMITY CARD READER.
	9	SECURITY BREAK GLASS UNIT (Green).
	9	MAGNETIC LOCK.
	6	DOME CCTV CAMERA.
	6	NEW CCTV CAMERA.
	3	CCTV CAMERA.
	1	CCTV CAMERA WITH PAN, TILT & ZOOM.
	1	INTERCOM

FOR TENDER

REV.	DATE.	DESCRIPTION.	BY.
------	-------	--------------	-----



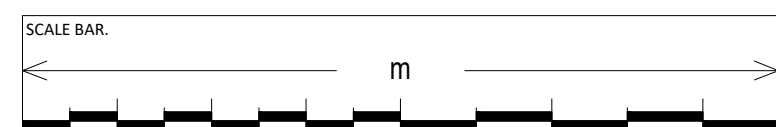
PROJECT:			
DTIC CAMPUS			
DETAILS:			
BLOCK C - GROUND FLOOR ACCESS CONTROL & CCTV LAYOUT			
DRAWN:	CHECKED:	INCEPTION DATE:	SCALE:
CP		2025.08.13	A1: 1:125
DRAWING NO.	DTI/C/GND/SEC/01		REV.
			A
PROJECT MANAGER NAME: NUMBER: EMAIL:		ACCOUNT MANAGER NAME: NUMBER: EMAIL:	

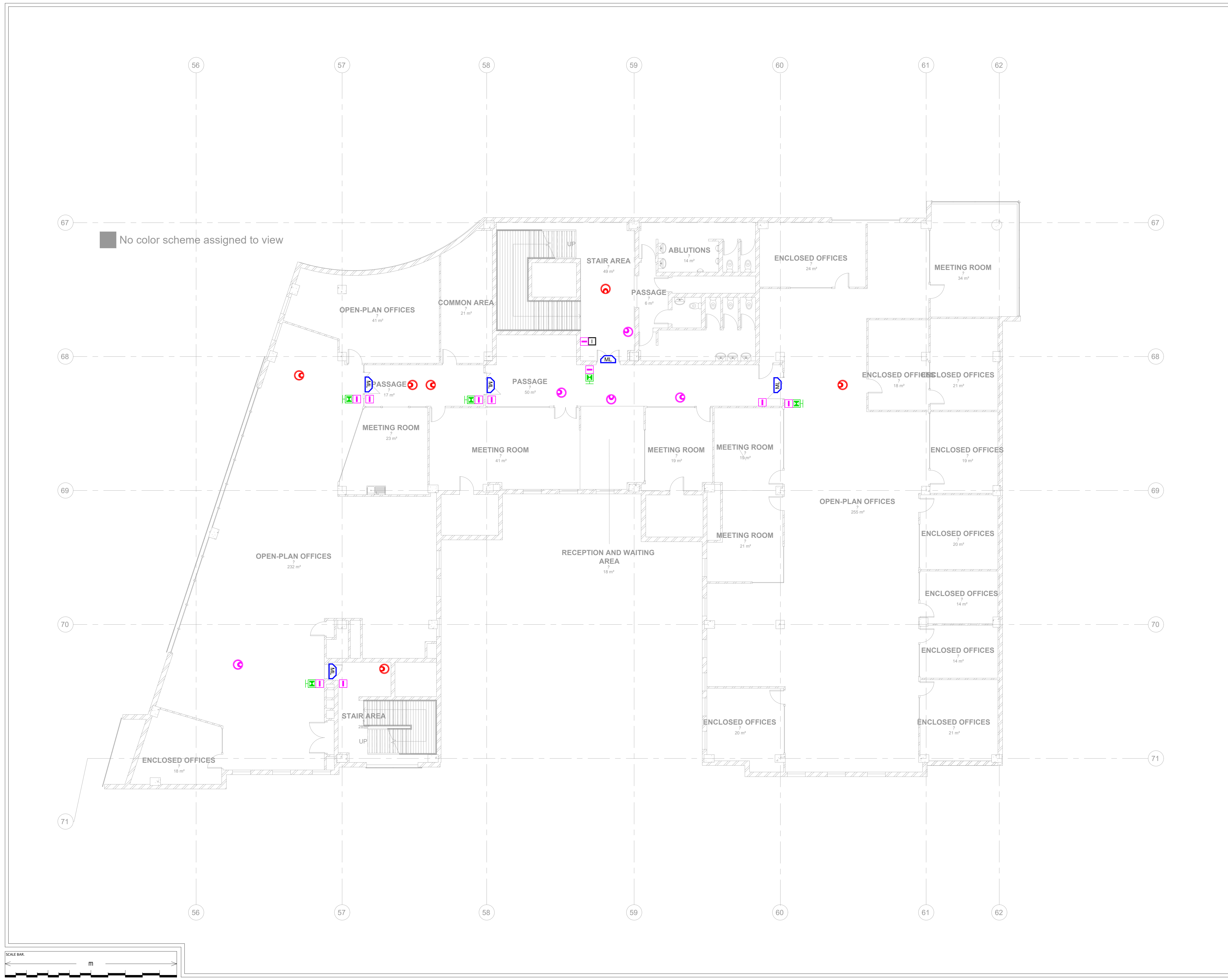


FOR TENDER



PROJECT MANAGER NAME: NUMBER: EMAIL:	ACCOUNT MANAGER NAME: NUMBER: EMAIL:
---	---





LEGEND		
Symbol	QTY	Description
	10	PROXIMITY CARD READER.
	5	SECURITY BREAK GLASS UNIT (Green).
	5	MAGNETIC LOCK.
	5	DOME CCTV CAMERA.
	6	NEW CCTV CAMERA.
	1	INTERCOM

FOR TENDER

REV.	DATE.	DESCRIPTION.	BY.
------	-------	--------------	-----



PROJECT:			
DTIC CAMPUS			
DETAILS:			
BLOCK D - SECOND FLOOR ACCESS CONTROL & CCTV LAYOUT			
DRAWN:	CHECKED:	INCEPTION DATE:	SCALE:
		2025.08.13	A1: 1:125
DRAWING NO.	DTI/D/2ND/SEC/01		REV.
			A
PROJECT MANAGER NAME: NUMBER: EMAIL:		ACCOUNT MANAGER NAME: NUMBER: EMAIL:	



LEGEND		
Symbol	QTY	Description
	12	PROXIMITY CARD READER.
	6	SECURITY BREAK GLASS UNIT (Green).
	6	MAGNETIC LOCK.
	5	DOME CCTV CAMERA.
	6	NEW CCTV CAMERA.
	2	INTERCOM

FOR TENDER

REV.	DATE.	DESCRIPTION.	BY.
------	-------	--------------	-----



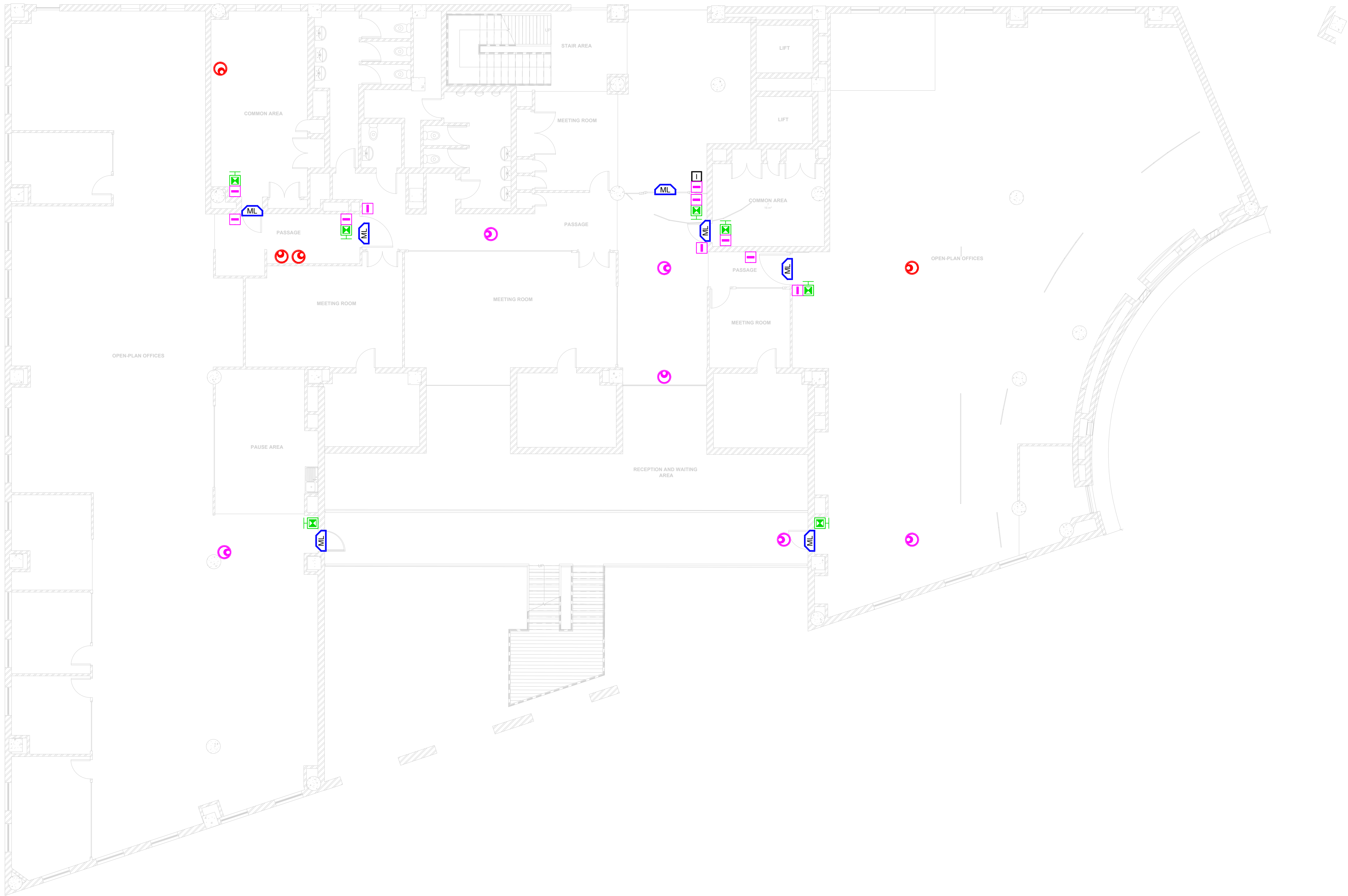
PROJECT:			
DTIC CAMPUS			
DETAILS:			
BLOCK D - THIRD FLOOR ACCESS CONTROL & CCTV LAYOUT			
DRAWN:	CHECKED:	INCEPTION DATE:	SCALE:
CP		2025.08.13	A1: 1:125
DRAWING NO.	DTI/D/3RD/SEC/01		REV.
			A
PROJECT MANAGER NAME: NUMBER: EMAIL:		ACCOUNT MANAGER NAME: NUMBER: EMAIL:	



LEGEND		
Symbol	QTY	Description
	4	PROXIMITY CARD READER.
	2	SECURITY BREAK GLASS UNIT (Green).
	2	MAGNETIC LOCK.
	6	DOME CCTV CAMERA.
	0	NEW CCTV CAMERA.
	3	CCTV CAMERA.
	1	NEW CCTV CAMERA.

FOR TENDER

REV.	DATE.	DESCRIPTION.	BY.
PROJECT: DTIC CAMPUS			
DETAILS: BLOCK D - GROUND FLOOR ACCESS CONTROL & CCTV LAYOUT			
DRAWN: CP	CHECKED:	INCEPTION DATE: 2025.08.13	SCALE: A1: 1:125
DRAWING NO. DTI/D/GND/SEC/01			REV. A
PROJECT MANAGER NAME: NUMBER: EMAIL:		ACCOUNT MANAGER NAME: NUMBER: EMAIL:	



LEGEND		
Symbol	QTY	Description
	10	PROXIMITY CARD READER.
	7	SECURITY BREAK GLASS UNIT (Green).
	7	MAGNETIC LOCK.
	6	DOMES CCTV CAMERA.
	4	NEW CCTV CAMERA.
	1	INTERCOM

FOR TENDER

REV.	DATE	DESCRIPTION	BY
------	------	-------------	----



PROJECT:			
DTIC CAMPUS			
DETAILS:			
BLOCK E - FIRST FLOOR ACCESS CONTROL & CCTV LAYOUT			
DRAWN:	CHECKED:	INCEPTION DATE:	SCALE:
CP		2025.08.13	A1: 1:125
DRAWING NO.			REV.
DTI/E/1ST/SEC/01			A
PROJECT MANAGER		ACCOUNT MANAGER	
NAME:		NAME:	
NUMBER:		NUMBER:	
EMAIL:		EMAIL:	



LEGEND		
Symbol	QTY	Description
	8	PROXIMITY CARD READER.
	6	SECURITY BREAK GLASS UNIT (Green).
	6	MAGNETIC LOCK.
	8	DOME CCTV CAMERA.
	4	NEW CCTV CAMERA.
	1	INTERCOM

FOR TENDER

REV.	DATE	DESCRIPTION	BY
------	------	-------------	----



PROJECT:			
DTIC CAMPUS			
DETAILS:			
BLOCK E - SECOND FLOOR ACCESS CONTROL & CCTV LAYOUT			
DRAWN: CP	CHECKED:	INCEPTION DATE: 2025.08.13	SCALE: A1: 1:125
DRAWING NO. DTI/E/2ND/SEC/01			REV. A
PROJECT MANAGER NAME: NUMBER: EMAIL:		ACCOUNT MANAGER NAME: NUMBER: EMAIL:	



LEGEND		
Symbol	QTY	Description
	10	PROXIMITY CARD READER.
	7	SECURITY BREAK GLASS UNIT (Green).
	7	MAGNETIC LOCK.
	6	DOME CCTV CAMERA.
	3	NEW CCTV CAMERA.
	1	INTERCOM

FOR TENDER

REV.	DATE	DESCRIPTION	BY
------	------	-------------	----



PROJECT:			
DTIC CAMPUS			
DETAILS:			
BLOCK E - THIRD FLOOR ACCESS CONTROL & CCTV LAYOUT			
DRAWN: CP	CHECKED:	INCEPTION DATE: 2025.08.13	SCALE: A1: 1:125
DRAWING NO. DTI/E/3RD/SEC/01			REV. A
PROJECT MANAGER NAME: NUMBER: EMAIL:		ACCOUNT MANAGER NAME: NUMBER: EMAIL:	



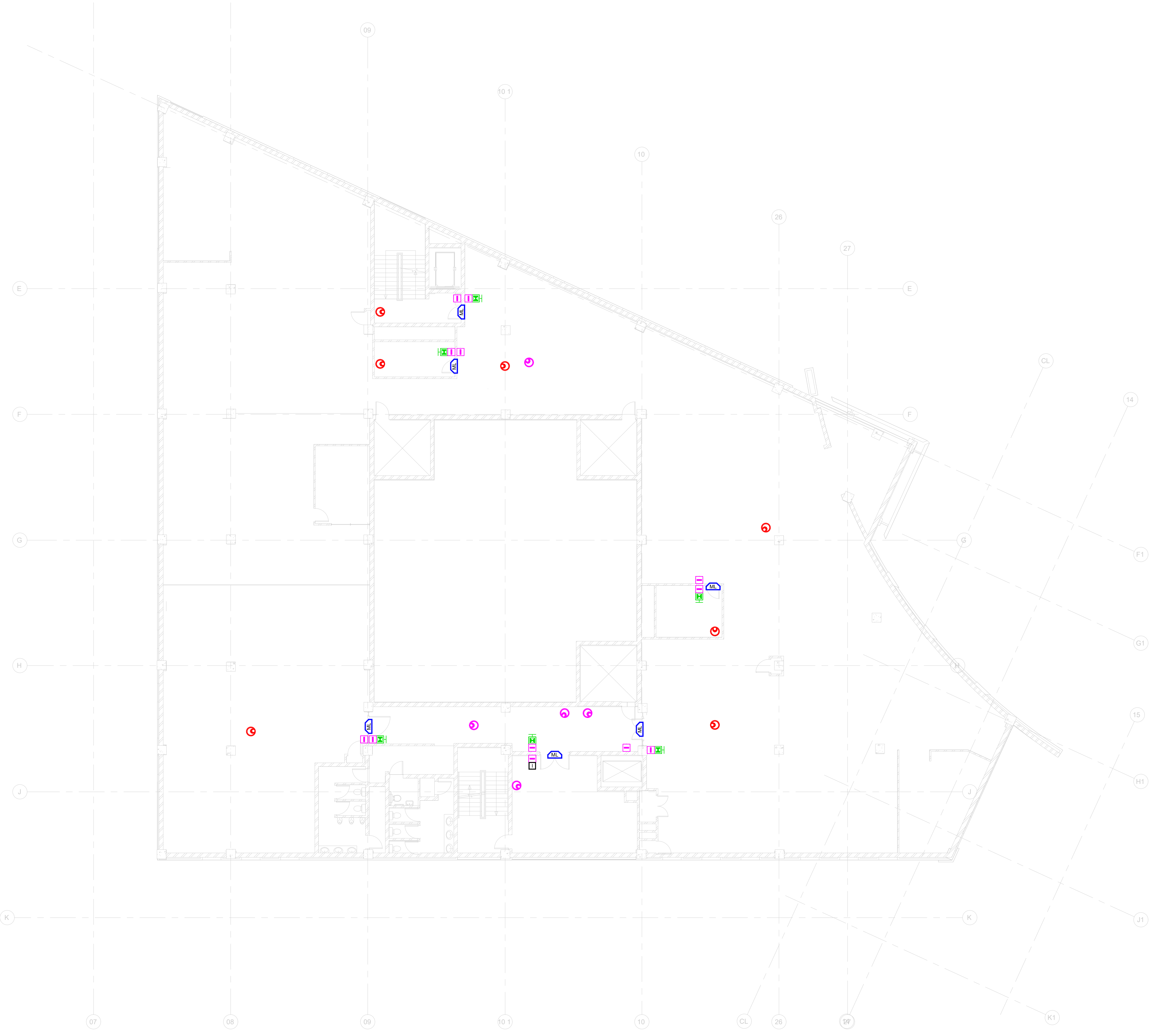
LEGEND		
Symbol	QTY	Description
	7	PROXIMITY CARD READER.
	5	SECURITY BREAK GLASS UNIT (Green).
	5	MAGNETIC LOCK.
	8	DOME CCTV CAMERA.
	4	NEW CCTV CAMERA.
	1	INTERCOM

FOR TENDER

REV.	DATE	DESCRIPTION	BY
------	------	-------------	----



PROJECT:			
DTIC CAMPUS			
DETAILS:			
BLOCK E - GROUND FLOOR ACCESS CONTROL & CCTV LAYOUT			
DRAWN: CP	CHECKED:	INCEPTION DATE: 2025.08.13	SCALE: A1: 1:125
DRAWING NO.: DTI/E/GND/SEC/01			REV.: A
PROJECT MANAGER NAME: NUMBER: EMAIL:		ACCOUNT MANAGER NAME: NUMBER: EMAIL:	



LEGEND		
Symbol	QTY	Description
	12	PROXIMITY CARD READER.
	6	SECURITY BREAK GLASS UNIT (Green).
	6	MAGNETIC LOCK.
	5	DOME CCTV CAMERA.
	7	NEW CCTV CAMERA.
	1	INTERCOM

FOR TENDER

REV.	DATE	DESCRIPTION	BY
------	------	-------------	----



PROJECT:			
DTIC CAMPUS			
DETAILS:			
BLOCK F - FIRST FLOOR ACCESS CONTROL & CCTV LAYOUT			
DRAWN: CP	CHECKED:	INCEPTION DATE: 2025.08.13	SCALE: A1: 1:125
DRAWING NO. DTI/F/1ST/SEC/01			REV. A
PROJECT MANAGER NAME: NUMBER: EMAIL:		ACCOUNT MANAGER NAME: NUMBER: EMAIL:	



LEGEND		
Symbol	QTY	Description
	8	PROXIMITY CARD READER.
	4	SECURITY BREAK GLASS UNIT (Green).
	4	MAGNETIC LOCK.
	5	DOME CCTV CAMERA.
	3	NEW CCTV CAMERA.
	1	INTERCOM

FOR TENDER

REV.

DATE.

DESCRIPTION.

BY.

PROJECT:

DTIC CAMPUS

DETAILS:

BLOCK F - SECOND FLOOR
ACCESS CONTROL & CCTV LAYOUT

DRAWN.

CP

CHECKED.

INCEPTION DATE.

2025.08.13

SCALE.

A1: 1:125

DRAWING NO.

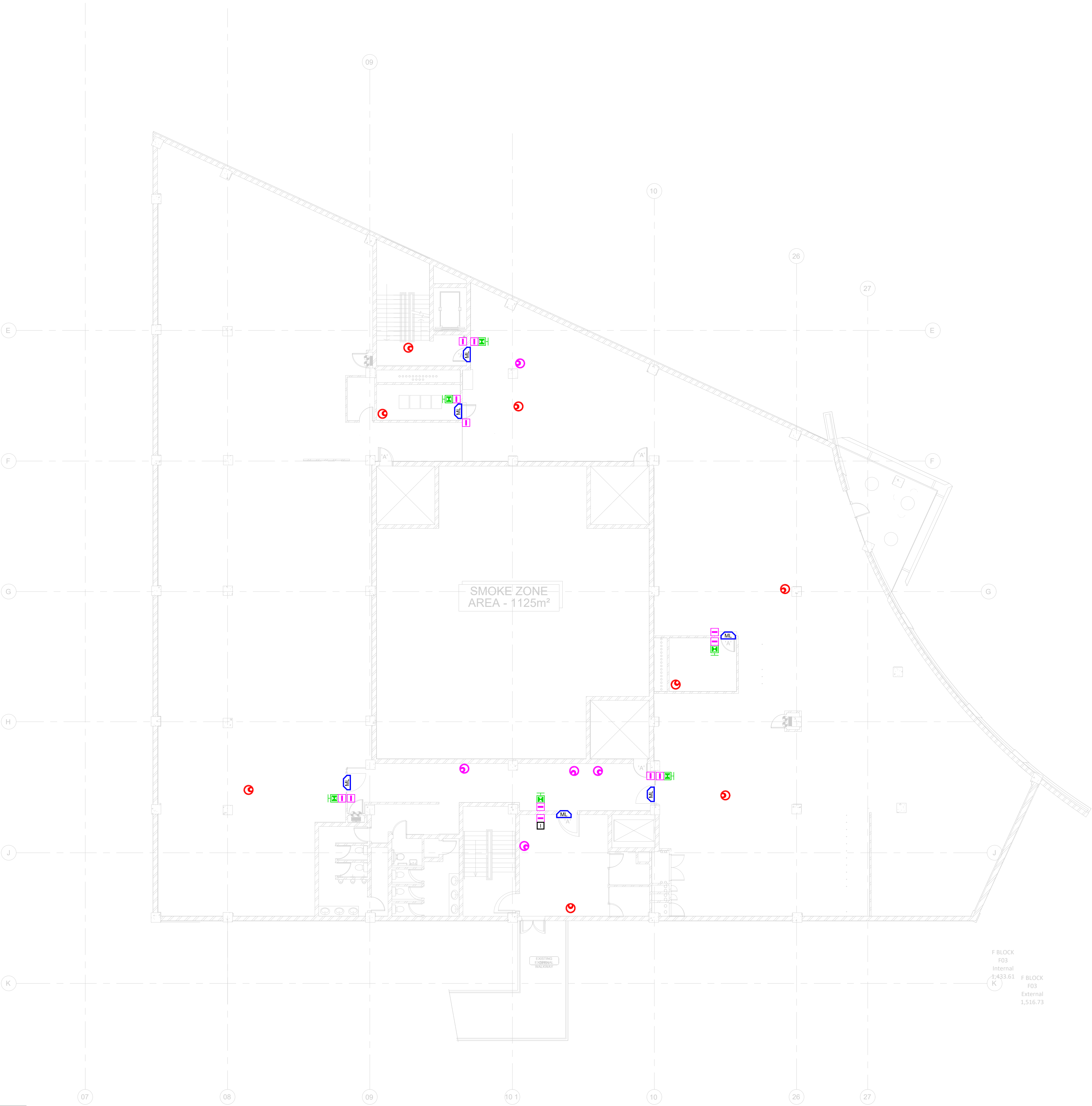
DTI/F/2ND/SEC/01

REV.

A

PROJECT MANAGER
NAME:
NUMBER:
EMAIL:

ACCOUNT MANAGER
NAME:
NUMBER:
EMAIL:



LEGEND		
Symbol	QTY	Description
	12	PROXIMITY CARD READER.
	6	SECURITY BREAK GLASS UNIT (Green).
	6	MAGNETIC LOCK.
	5	DOME CCTV CAMERA.
	8	NEW CCTV CAMERA.
	1	INTERCOM

FOR TENDER

REV.	DATE	DESCRIPTION	BY
------	------	-------------	----



PROJECT:			
DTIC CAMPUS			
DETAILS:			
BLOCK F - THIRD FLOOR ACCESS CONTROL & CCTV LAYOUT			
DRAWN.	CHECKED.	INCEPTION DATE.	SCALE.
CP		2025.08.13	A1: 1:125
DRAWING NO.			REV.
DTI/F/3RD/SEC/01			A
PROJECT MANAGER		ACCOUNT MANAGER	
NAME:		NAME:	
NUMBER:		NUMBER:	
EMAIL:		EMAIL:	

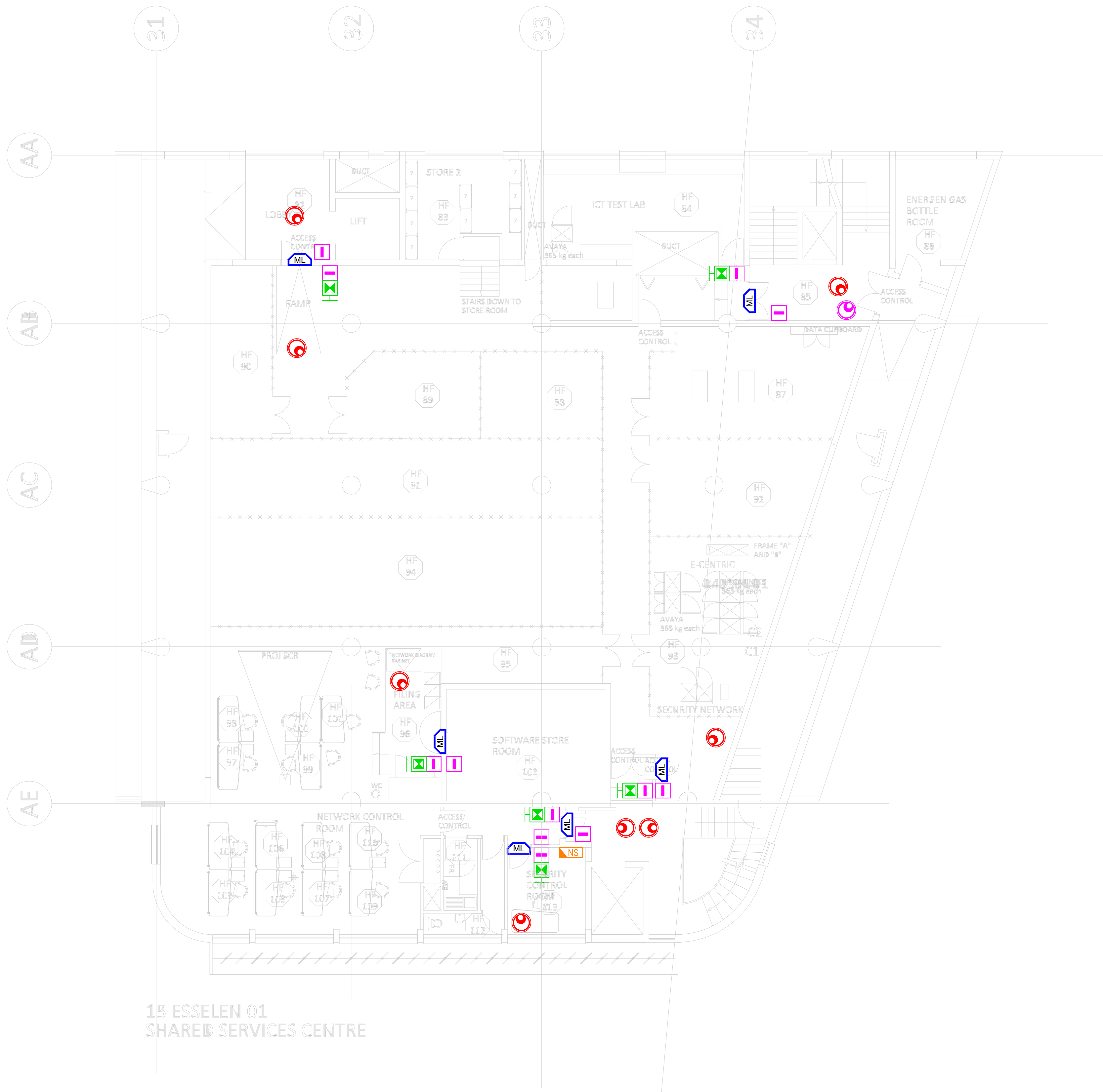


LEGEND		
Symbol	QTY	Description
	13	PROXIMITY CARD READER.
	6	SECURITY BREAK GLASS UNIT (Green).
	6	MAGNETIC LOCK.
	7	DOME CCTV CAMERA.
	6	NEW CCTV CAMERA.
	1	NO TOUCH EXIT BUTTON.

REV.	DATE	DESCRIPTION	BY
------	------	-------------	----



PROJECT:			
DTIC CAMPUS			
DETAILS:			
BLOCK F - GROUND FLOOR ACCESS CONTROL & CCTV LAYOUT			
DRAWN.	CHECKED.	INCEPTION DATE.	SCALE.
CP		2025.08.13	A1: 1:125
DRAWING NO.			REV.
DTI/F/GND/SEC/01			A
PROJECT MANAGER		ACCOUNT MANAGER	
NAME:		NAME:	
NUMBER:		NUMBER:	
EMAIL:		EMAIL:	



13 ESSELEN 01
SHARED SERVICES CENTRE

LEGEND		
Symbol	QTY	Description
	12	PROXIMITY CARD READER.
	6	SECURITY BREAK GLASS UNIT (Green).
	6	MAGNETIC LOCK.
	1	DOMES CCTV CAMERA.
	1	NETWORK SWITCH.
	8	NEW CCTV CAMERA.

FOR TENDER

REV.	DATE	DESCRIPTION	BY
------	------	-------------	----



PROJECT:

DTIC CAMPUS

DETAILS:

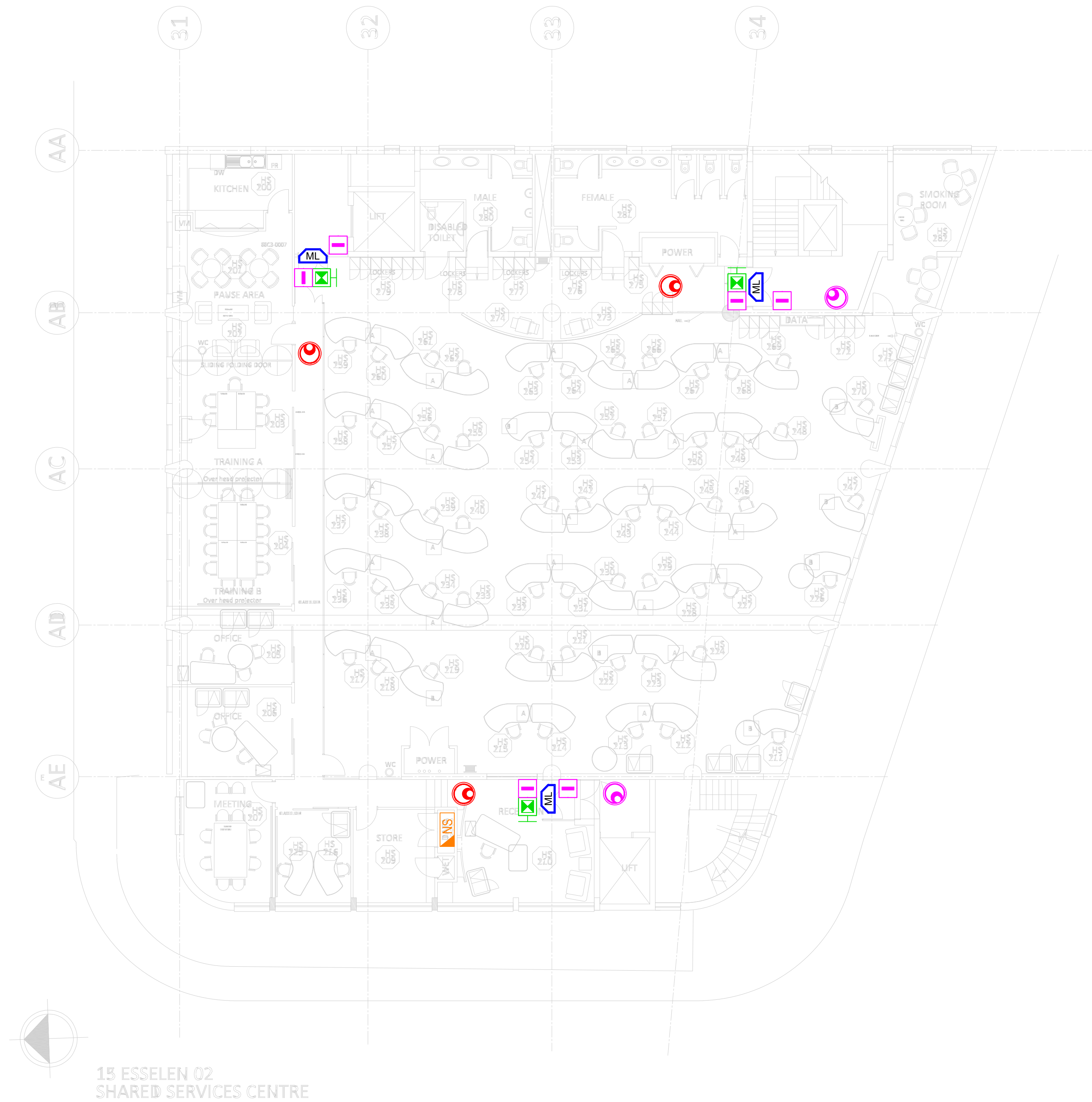
SSC BUILDING - FIRST FLOOR
ACCESS CONTROL & CCTV LAYOUT

DRAWN	CHECKED	INCEPTION DATE	SCALE
CP		2025.08.13	A1: 1:125

DRAWING NO.	REV.
DTI/SSC/1ST/SEC/01	A

PROJECT MANAGER	ACCOUNT MANAGER
NAME:	NAME:
NUMBER:	NUMBER:
EMAIL:	EMAIL:





LEGEND		
Symbol	QTY	Description
	6	PROXIMITY CARD READER.
	3	SECURITY BREAK GLASS UNIT (Green).
	3	MAGNETIC LOCK.
	2	DOMI CCTV CAMERA.
	1	NETWORK SWITCH.
	3	NEW CCTV CAMERA.

FOR TENDER

REV.	DATE	DESCRIPTION	BY
------	------	-------------	----



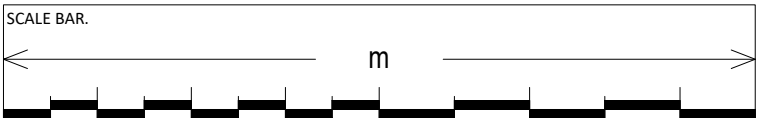
PROJECT: DTIC CAMPUS

DETAILS: SSC BUILDING - SECOND FLOOR
ACCESS CONTROL & CCTV LAYOUT

DRAWN	CHECKED	INCEPTION DATE	SCALE
CP		2025.08.13	A1: 1:75

DRAWING NO.	REV.
DTI/SSC/2ND/SEC/01	A

PROJECT MANAGER	ACCOUNT MANAGER
NAME:	NAME:
NUMBER:	NUMBER:
EMAIL:	EMAIL:





13 ESSELEN 03
SHARED SERVICES CENTRE

LEGEND		
Symbol	QTY	Description
	10	PROXIMITY CARD READER.
	5	SECURITY BREAK GLASS UNIT (Green).
	5	MAGNETIC LOCK.
	1	DOM E CCTV CAMERA.
	1	NETWORK SWITCH.
	6	NEW CCTV CAMERA.

FOR TENDER

REV.	DATE.	DESCRIPTION.	BY.
------	-------	--------------	-----



PROJECT:			
DTIC CAMPUS			
DETAILS:			
SSC BUILDING - THIRD FLOOR ACCESS CONTROL & CCTV LAYOUT			
DRAWN: CP	CHECKED:	INCEPTION DATE: 2025.08.13	SCALE: A1: 1:75
DRAWING NO.: DTI/SSC/3RD/SEC/01			REV.: A
PROJECT MANAGER NAME: NUMBER: EMAIL:		ACCOUNT MANAGER NAME: NUMBER: EMAIL:	



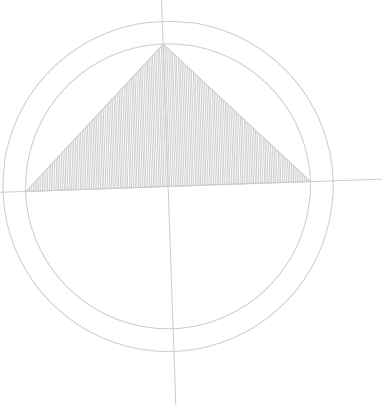
LEGEND		
Symbol	QTY	Description
	9	PROXIMITY CARD READER.
	4	SECURITY BREAK GLASS UNIT (Green).
	4	MAGNETIC LOCK.
	3	DOME CCTV CAMERA.
	6	NEW CCTV CAMERA.

FOR TENDER

REV.	DATE	DESCRIPTION	BY
------	------	-------------	----



PROJECT:			
DTIC CAMPUS			
DETAILS:			
SSC BUILDING - BASEMENT LEVEL ACCESS CONTROL & CCTV LAYOUT			
DRAWN:	CHECKED:	INCEPTION DATE:	SCALE:
CP		2025.08.13	A1: 1:125
DRAWING NO.			REV.
DTI/SSC/BMT/SEC/01			A
PROJECT MANAGER		ACCOUNT MANAGER	
NAME:		NAME:	
NUMBER:		NUMBER:	
EMAIL:		EMAIL:	



15 ESSELEN 00
SHARED SERVICES CENTRE

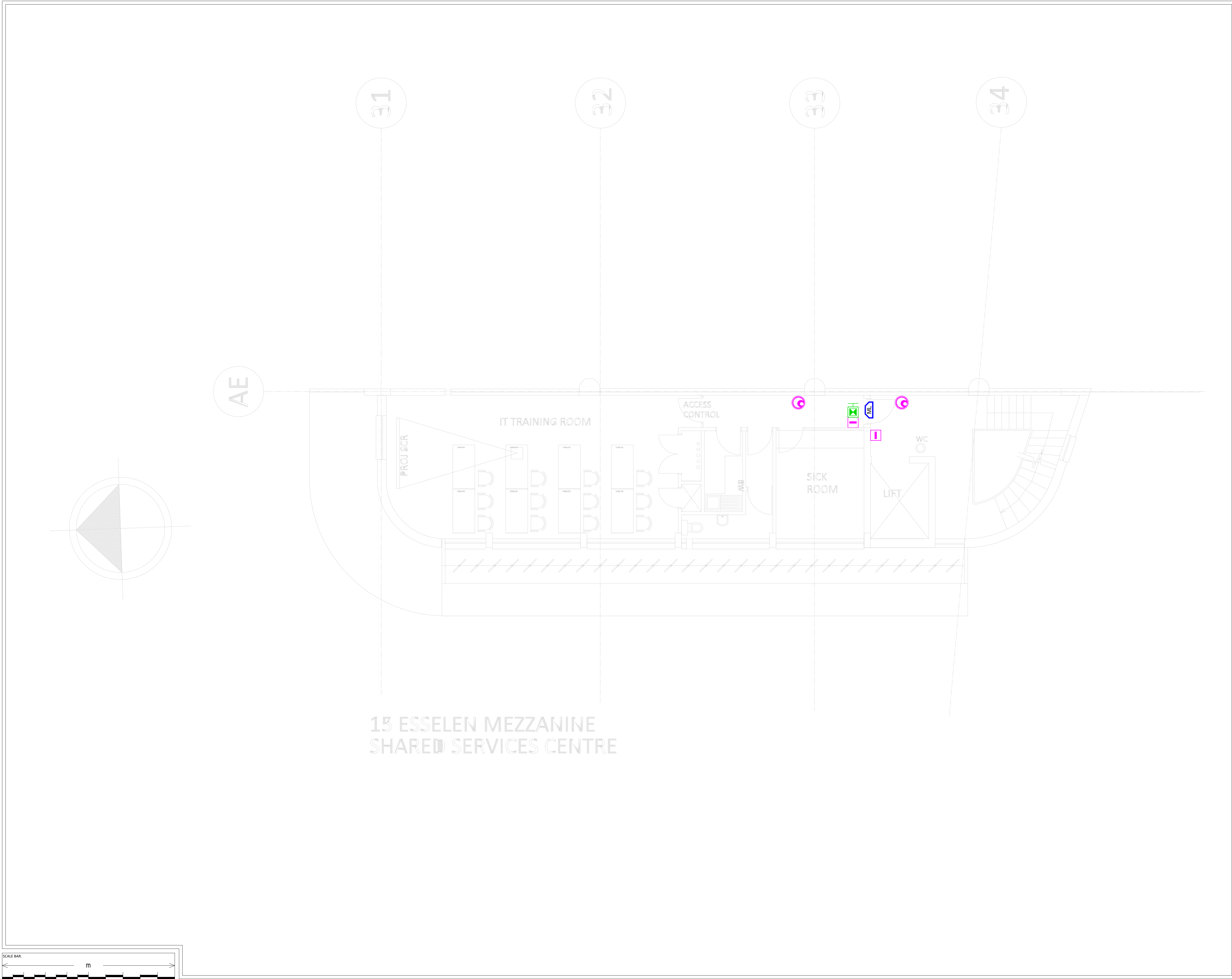


LEGEND		
Symbol	QTY	Description
	20	PROXIMITY CARD READER.
	11	SECURITY BREAK GLASS UNIT (Green).
	10	MAGNETIC LOCK.
	1	DOME CCTV CAMERA.
	1	NETWORK SWITCH.
	15	NEW CCTV CAMERA.

REV.	DATE	DESCRIPTION	BY
------	------	-------------	----



PROJECT:			
DTIC CAMPUS			
DETAILS:			
SSC BUILDING - GROUND FLOOR ACCESS CONTROL & CCTV LAYOUT			
DRAWN: CP	CHECKED:	INCEPTION DATE: 2025.08.13	SCALE: A1: 1:125
DRAWING NO. DTI/SSC/GND/SEC/01	REV. A		
PROJECT MANAGER NAME: NUMBER: EMAIL:		ACCOUNT MANAGER NAME: NUMBER: EMAIL:	



13 ESSELEN MEZZANINE
SHARED SERVICES CENTRE

LEGEND		
Symbol	QTY	Description
	2	PROXIMITY CARD READER.
	1	SECURITY BREAK GLASS UNIT (Green).
	1	MAGNETIC LOCK.
	2	DOME CCTV CAMERA.

FOR TENDER

REV.	DATE	DESCRIPTION	BY
------	------	-------------	----



PROJECT:
DTIC CAMPUS

DETAILS:
SSC BUILDING - MEZZANINE FLOOR
ACCESS CONTROL & CCTV LAYOUT

DRAWN. CP	CHECKED.	INCEPTION DATE. 2025.08.13	SCALE. A1: 1:75
DRAWING NO. DTI/SSC/MEZ/SEC/01			REV. A

PROJECT MANAGER NAME: NUMBER: EMAIL:	ACCOUNT MANAGER NAME: NUMBER: EMAIL:
---	---