

1. PURPOSE

The purpose of this Scope of Work (SOW) is to define the requirements for the procurement of a Visitor Management System (VMS) software solution, including all necessary licensing, that is specifically designed to operate on the University's existing and future Chainway C66 handheld devices and integrate seamlessly with the Gallagher access control platform.

This SOW outlines the specific software, licensing, hardware support, and services required from the successful service provider to ensure the implementation of a modern, integrated, and secure VMS solution across all University campuses.

Technical Security Solutions (TSS), operating under Campus Protection Services (CPS), is responsible for overseeing this project and its integration into the University's security ecosystem. The VMS software will be deployed on the University's existing Chainway C66 handheld devices, enabling mobile visitor management capabilities. The solution must integrate fully with the Gallagher Command Centre access control platform and provide robust functionality for managing exams, graduations, and other high-volume events. The seamless operation of the VMS is essential for maintaining campus safety, operational efficiency, and regulatory compliance.

The objective of acquiring this VMS is to satisfy the following:

- To provide a safe and secure environment for the University community by ensuring all visitors are properly registered, vetted, and tracked using mobile handheld devices.
- To leverage existing University hardware investment by deploying VMS software on the Chainway C66 handheld devices already in operation.
- To automate and streamline visitor management processes, improving operational efficiency and reducing administrative burden on staff.
- To maintain accurate, auditable digital visitor records, ensuring compliance with the Protection of Personal Information Act (POPIA).
- To improve the visitor experience through mobile pre-registration, QR code scanning, and automatic host notifications.
- To enable real-time visitor tracking and emergency roll-call capability to support incident response and business continuity.
- To integrate the VMS with the Gallagher access control platform for seamless visitor credential management and access rights assignment.
- To provide event management capabilities specifically designed for exams, graduations, conferences, and any other University requirements.

- To ensure continuity of hardware support through the supply of replacement Chainway C66 handheld devices.

2. THE UNIVERSITY'S OBJECTIVES

The University seeks to appoint a qualified service provider through an open competitive tender process to provide a comprehensive Visitor Management System (VMS), including all necessary hardware, software, licensing, installation, and ongoing support.

- The successful service provider shall deliver:

2.1 Software Licensing Requirements

The Supplier must provide all necessary software licenses for the VMS solution, including:

License Type	Description	Requirement
VMS Core Software License	Core Visitor Management System software license enabling all core functionality.	Mandatory
Mobile Device License	Licenses for deployment on Chainway C66 handheld devices (minimum XX units).	Mandatory
Gallagher Integration License	Licenses required for REST API integration with Gallagher Command Centre.	Mandatory
Event Management License	Licenses for event management functionality (exams, graduations, conferences, etc.).	Mandatory
Server/Backend License	Server-side licensing for VMS backend and database.	Mandatory
User/Administrator Licenses	Licenses for system administrators and users.	Mandatory

License Type	Description	Requirement
API Integration Licenses	Licenses for integration with other University systems as required.	Mandatory

2.2 Chainway C66 Hardware Requirements

The VMS software must be fully compatible with the University's existing Chainway C66 handheld devices:

Hardware Feature	Requirement
Operating System	Must support Android 11 or 13 (Chainway C66 runs on Android 11/13).
Display	Must support 5.5-inch HD display (1440 x 720 resolution).
Scanner Integration	Must utilise built-in 2D barcode scanner (Zebra SE4710/SE2100 or equivalent) for QR code scanning.
NFC Functionality	Must utilise built-in NFC for contactless visitor check-in/out.
Camera	Must utilise built-in 13MP camera for visitor photo capture.
Connectivity	Must support Wi-Fi, 4G/LTE, and Bluetooth connectivity.
Battery	Must be optimised for battery life (5200mAh battery, >12 hours continuous use).
SDK	Must be compatible with Chainway Software Development Kit (SDK).

2.3 Hardware Support and Replacement

The University currently owns a fleet of Chainway C66 handheld devices used for access control and visitor management functions. To ensure continuity of operations and maintain the mobile visitor management capability, the Supplier must provide comprehensive hardware support:

Hardware Support Requirement	Description	Requirement
Device Repairs	The Supplier must provide repair services for faulty Chainway C66 devices.	Mandatory
Replacement Devices	The Supplier must supply replacement Chainway C66 handheld devices or equivalent when devices are beyond repair or to expand the fleet.	Mandatory
Loaner Devices	The Supplier must provide loaner devices during the repair period to ensure uninterrupted operations.	Mandatory
Warranty Support	All replacement devices must carry a minimum 12-month warranty.	Mandatory
Spare Parts	The Supplier must maintain an inventory of spare parts for the Chainway C66 devices.	Mandatory
Firmware Updates	The Supplier must provide firmware updates for the Chainway C66 devices as required.	Mandatory
Technical Support	The Supplier must provide technical support for the Chainway C66 devices and software.	Mandatory

Hardware Support Requirement	Description	Requirement
Device Configuration	The Supplier must pre-configure replacement devices with the VMS software before delivery to the University.	Mandatory

2.4 Gallagher Access Control Integration

The VMS software must integrate seamlessly with the University's existing Gallagher access control platform.

2.4.1 Integration Requirements

Integration Feature	Description	Requirement
Visitor Credential Management	Create, manage, and revoke visitor credentials within Gallagher Command Centre.	Mandatory
REST API Integration	Integrate via Gallagher Command Centre REST API for secure data exchange.	Mandatory
Cardholder Synchronisation	Synchronise visitor cardholder data with Gallagher Command Centre Cardholder database.	Mandatory
Automatic Access Rights Assignment	Automatically assign access rights in Gallagher based on visitor profile, host, and destination.	Mandatory
Real-Time Access Control	Grant real-time access to designated doors, gates, and turnstiles based on VMS registration.	Mandatory
QR Code Integration	QR codes generated by VMS scannable at Gallagher-integrated readers for access.	Mandatory

Integration Feature	Description	Requirement
Visitor Photo Synchronisation	Visitor photos synchronised with Gallagher for verification purposes.	Mandatory
Visitor Tracking	Real-time visibility of visitor movements via Gallagher integration.	Mandatory
Audit Trail	Visitor access events logged and synchronised with VMS for complete audit trail.	Mandatory
Emergency Lockdown Integration	Revoke all visitor access rights during emergency lockdown.	Mandatory
Two-Way Synchronisation	Real-time two-way data synchronisation between VMS and Gallagher.	Mandatory
Multi-Site Support	Support all University campuses and locations where Gallagher is deployed.	Mandatory
Visitor Badge Printing Integration	Integrate with Gallagher badge printing functionality for visitor badges.	Mandatory

2.5 Event Management Requirements

The VMS software must provide comprehensive event management capabilities specifically designed for exams, graduations, conferences, and any other University requirements:

Event Feature	Description	Requirement
Event Creation	Create and manage unlimited events (exams, graduations, conferences, open days, campus tours, etc.).	Mandatory
Event Types	Support multiple event types with customisable workflows.	Mandatory
Pre-Registration	Share secure registration links with guests for pre-registration.	Mandatory
Digital Ticketing	Send digital tickets with unique QR codes to attendees.	Mandatory
Batch Processing	Batch print visitor badges and process large visitor volumes.	Mandatory
Capacity Management	Configure capacity limits and manage attendance numbers.	Mandatory
Waitlist Management	Manage waitlists when events reach capacity.	Mandatory
Pre-Screening	Screen attendees against watchlists during registration.	Mandatory
Mobile Check-In Stations	Set up mobile check-in stations anywhere on campus using Chainway C66 devices.	Mandatory
Multi-Event Support	Manage multiple events simultaneously across different campuses.	Mandatory

Event Feature	Description	Requirement
Exam Management	Specialised functionality for exam invigilation and candidate verification.	Mandatory
Graduation Management	Specialised functionality for graduation ceremonies (multiple sessions, guest management, etc.).	Mandatory
Conference Management	Conference and seminar management with session tracking.	Mandatory
Reporting	Generate event-specific reports (attendance, waitlists, no-shows, etc.).	Mandatory
Export Functionality	Export event data to Excel, PDF, and other formats.	Mandatory
Historical Event Data	Maintain and provide access to historical event data.	Mandatory
Guest Management	Manage guest lists, plus-ones, and attendee details.	Mandatory
Vendor/Exhibitor Management	Manage vendors and exhibitors at events.	Mandatory
Parking Management	Manage visitor parking for events.	Mandatory
Event Badges	Customise and print event-specific visitor badges.	Mandatory
Check-in/out Dashboard	Real-time dashboard showing event check-in/out statistics.	Mandatory

Event Feature	Description	Requirement
Email Notifications	Automated email notifications for event registration, reminders, and confirmations.	Mandatory
SMS Notifications	SMS notifications for event reminders and updates.	Mandatory

2.6 Additional University Requirements

The VMS software must be capable of handling any additional visitor management requirements of the University:

Additional Requirement	Description	Requirement
Contractor Management	Track and manage contractors working on campus.	Mandatory
Delivery Management	Manage delivery drivers and couriers.	Mandatory
Student Visitor Management	Track student visitors to residences and academic buildings.	Mandatory
VIP Management	Manage VIP visitors with enhanced privacy and security.	Mandatory
Watchlist Integration	Screen visitors against watchlists and blacklists.	Mandatory
Emergency Rollcall	Generate emergency roll-call reports for evacuation or lockdown situations.	Mandatory

Additional Requirement	Description	Requirement
Visitor History	Maintain comprehensive visitor history for audit and investigation purposes.	Mandatory
Custom Fields	Create custom visitor fields as required.	Mandatory
Whitelist/Blacklist Management	Manage whitelists and blacklists for visitor access.	Mandatory
Multi-Campus Support	Support all University campuses and locations.	Mandatory
Multi-Language Support	Support multiple languages as required.	Mandatory

3. SCOPE OF WORK

The successful service provider (Supplier) shall perform the following duties as part of the VMS software procurement, licensing, hardware support, and implementation:

3.1 Software Licensing Provisioning

- The Supplier must provide valid, up-to-date software licenses for the VMS solution for the duration of the contract.
- The Supplier must provide all necessary licenses for deployment on the University's Chainway C66 handheld devices.
- The Supplier must provide all necessary licenses for integration with Gallagher Command Centre (REST API Cardholders, View Events & Alarms, Create Events & Alarms licenses as required).
- The Supplier must provide event management licenses for exams, graduations, conferences, and all other event types.
- The Supplier must ensure that all licensing is compliant with OEM requirements and University policies.

- The Supplier must provide clear documentation on licensing terms, renewal schedules, and costs.
- The Supplier must provide remote management software license.

3.2 Software Configuration:

- The Supplier must configure the VMS software in accordance with the University's requirements.
- The Supplier must configure the software for deployment on Chainway C66 handheld devices, including:
 - Visitor registration workflows.
 - Pre-registration portals.
 - Host notification settings.
 - QR code generation and scanning.
 - Event management configurations for all event types.
 - Reporting and dashboard configurations.
 - ID, Drivers and Passport decryption Licensing
- The Supplier must configure the software for the University's specific event requirements:
 - Exam management workflows.
 - Graduation ceremony workflows.
 - Conference management workflows.
 - Open day and campus tour workflows.

3.3 Gallagher Access Control Integration

- The Supplier must integrate the VMS software with the Gallagher Command Centre platform.
- The Supplier must use Gallagher REST APIs for integration.
- The Supplier must provide documentation of the integration methodology and APIs used.
- The Supplier must conduct comprehensive integration testing with the Gallagher system prior to go-live.
- The Supplier must provide a detailed Integration Test Plan and Test Results Report.

- The integration must be formally signed off by the University's ICT Director and CPS Director before the system is accepted.
- The Supplier must ensure that the integration supports all University campuses and locations.

3.4 Chainway C66 Device Support:

- The Supplier must provide the VMS software pre-installed and configured on Chainway C66 devices.
- The Supplier must provide repair services for faulty Chainway C66 devices.
- The Supplier must supply replacement Chainway C66 or newly released replacement model handheld devices when devices are beyond repair or to expand the fleet.
- All replacement devices must carry a minimum 12-month warranty.
- The Supplier must maintain an inventory of spare parts for the Chainway C66 devices.
- The Supplier must provide firmware updates for the Chainway C66 devices as required.
- The Supplier must pre-configure replacement devices with the VMS software before delivery to the University.
- The Supplier must provide ongoing technical support for the Chainway C66 devices and software.

3.5 Training and Knowledge Transfer:

- The Supplier must provide comprehensive training for CPS and ICT personnel on:
 - System administration.
 - User management.
 - Chainway C66 device configuration, deployment, and troubleshooting.
 - Reporting and analytics.
 - Software maintenance and troubleshooting.
 - Configuration and customisation.
 - Event management configuration for all event types.
- The Supplier must provide system documentation and operational manuals.
- The Supplier must conduct knowledge transfer sessions during the transition and contract commencement phases.

3.6 Data Integrity and Security:

- The Supplier must ensure that the VMS, including all hardware and software, complies with the Protection of Personal Information Act (POPIA).
- The Supplier must ensure the security of all personal data processed by the VMS.
- The Supplier must implement appropriate security measures, including:
 - Role-based access control.
 - Data encryption (at rest and in transit).
 - Secure data storage and backup.
 - Audit trails for all system activity.
- The Supplier must ensure that system configurations remain accessible to the University to avoid vendor lock-in.

4. ROUTINE AND BREAKDOWN MAINTENANCE

The Supplier shall perform routine and breakdown maintenance for the VMS software and Chainway C66 devices in accordance with the following:

4.1 Routine Maintenance

- The Supplier must perform routine maintenance in accordance with:
 - The original equipment manufacturer's technical specifications, warranties, and recommendations.
- The Supplier must provide a preventative maintenance schedule for all software and hardware within 30 days of contract award.
- The Supplier must inform the University's TSS help desk of all additional maintenance or upgrade work requirements as identified during the contract term.
- The Supplier must perform preventative maintenance on Chainway C66 devices as required

4.2 Breakdown Maintenance

- The Supplier must perform breakdown maintenance in accordance with calls logged at TSS.
- The Supplier must respond to and resolve breakdown incidents within the timeframes specified in the SLA.
- The Supplier must provide a comprehensive report for each maintenance task, including a summary of work performed, issues resolved, and parts replaced.

4.3 Reporting

- The Supplier must provide a comprehensive report for each maintenance task during a specific month by completing the University's service record.
- The Supplier must furnish the University with reports in electronic format by no later than the 10th (tenth) day of the month following the month to which the report relates.

4.4 Compliance

- The Supplier must ensure complete compliance with all University OHS and ICT requirements, including ensuring the safe and correct execution of all services performed remotely or on-site.

5. STANDARDS

The Supplier always guarantees adherence to all applicable standards and regulations:

5.1 Data Protection

- The Supplier must comply with the Protection of Personal Information Act (POPIA) and University data governance policies.
- The Supplier must ensure the security of all personal data processed by the VMS.

5.2 Security Standards

- The Supplier must maintain the security of the application, ensuring that it is protected against known vulnerabilities.
- The Supplier must comply with University ICT security standards.

5.3 Chainway C66 Compatibility

- The VMS software must be fully compatible with Chainway C66 Android 11/13 operating system.
- The Supplier must provide compatibility with both existing and future Chainway C66 devices.

5.4 Gallagher Integration Standards

- The VMS software must integrate with Gallagher Command Centre v8.90 and above.
- The VMS software must use Gallagher REST APIs for secure integration.

5.4 Quality Standards

- The Supplier must ensure that all new goods and services are fit for purpose.
- The Supplier must ensure that all installations are of high quality and meet the University's expectations.

6. SERVICES LEVELS

The Supplier must ensure full-time availability (365 days x 24 hours) via a reliable call-out system for critical system failures. The following service level standards will apply:

6.1 Service Level Standards

Service	Service Level Standards	Penalty / Service Level Credit Applied
Software Licensing	All licensing must be active and valid for the duration of the contract.	Not applicable (this is a fundamental requirement).
Hardware Warranty	All hardware must have a minimum 3-year OEM warranty with next-business-day response.	Not applicable.
Critical System Failure	Response Time: Within 1 hour (24/7). Resolution Time: Within 4 hours (24/7).	R2,000 per hour per incident for failure to meet response or resolution times.
Major System Failure	Response Time: Within 2 hours (24/7). Resolution Time: Within 8 hours (24/7).	R2,000 per hour per incident for failure to meet response or resolution times.
General Issues	Response Time: Within 4 hours (24/7). Resolution Time: By the Next Business Day.	R1,000 per hour per incident for failure to meet response or resolution times.
Software Updates	All critical security and feature updates must be provided within 5 business days of their release.	R5,000 per incident.

Gallagher Integration Failure	Response Time: Within 1 hour (24/7). Resolution Time: Within 4 hours (24/7).	R5,000 per hour per incident for failure to meet response or resolution times.
-------------------------------------	---	--

6.2 Escalation Procedures.

The following escalation procedures will be used when dealing with performance-related matters and penalties:

Escalation Situation	Process	Responsible Parties
1st Escalation	The University will issue a penalty notice.	University Representative
2nd Escalation	Acknowledgement of the penalty within 2 (two) days.	Supplier
3rd Escalation	The credit note shall be sent to the University.	Supplier
4th Escalation	Penalties will be deducted from the relevant invoice.	University Representative

6.3 Incident Closure

Once a service problem or incident is deemed resolved by the Supplier, the University contact person will receive an email requesting acknowledgement that the incident may now be closed. If the University is not satisfied, the incident will remain open until both parties agree on completion.

7. WARRANTY

The Supplier is responsible for ensuring that all new hardware, software, and licensing are fit for purpose.

7.1 Licensing Warranty

- The Supplier warrants that the software licenses provided are genuine, valid, and will remain active for the entire contract term.
- The Supplier warrants that the software will perform in accordance with its intended purpose and specifications.

7.2 Gallagher Integration Warranty

- The Supplier warrants that the VMS-Gallagher integration will function as specified in Section 2.4 of this Scope of Work.
- The Supplier warrants that the integration will be maintained and supported for the duration of the contract.
- The Supplier warrants that any future updates to the Gallagher system will be supported by the VMS integration.
- The Supplier warrants that the integration will not compromise the security or performance of the Gallagher access control platform.

7.3 Chainway C66 Compatibility and Hardware Warranty

- The Supplier warrants that the VMS software will operate optimally on the Chainway C66 handheld devices.
- The Supplier warrants that the software will utilise the device's full capabilities (scanner, camera, NFC, etc.).
- The Supplier warrants that replacement devices will be genuine Chainway C66 devices and must carry a minimum 12-month warranty.
- The Supplier warrants that repairs will be completed using genuine spare parts.

7.4 Event Management Warranty

- The Supplier warrants that the event management functionality will support all event types required by the University, including exams, graduations, conferences, open days, and campus tours.
- The Supplier warrants that the software will handle the expected visitor volumes during peak events.

7.5 Support Warranty

- The Supplier warrants that it will provide technical support and software updates in accordance with the service levels defined in Section 6 of this Scope of Work.

- The Supplier warrants that it will provide hardware support in accordance with the service levels defined in Section 6 of this Scope of Work

8. CONTRACTUAL MANAGEMENT

8.1 Service Review Meetings:

- Service review meetings will be held at a frequency agreed upon by both parties, but not less than once every month.
- The issues to be addressed at such meetings will include:
 - Service performance levels.
 - Support performance levels.
 - System issues and software performance.
 - Gallagher integration performance.
 - Chainway C66 device performance and support.
 - Event management performance.
 - Administrative issues.
 - Proposed changes or upgrades.
 - Incident management report.

8.2 Reporting:

- The Supplier must furnish the University with reports in electronic format substantially in accordance with the specifications listed by the University by no later than the 10th (tenth) day of the month following the month to which the report relates.
- The University shall keep formal minutes of all such meetings and circulate these among the attendees.
- It is also the responsibility of the Supplier to keep on file and make available for inspection by the University's appointed administrator or auditor the statistics, minutes, and other records required by University policy.

8.3 Annual Review Process:

- The University will perform a bi-annual review of the Supplier's performance.
- The Supplier's mid-year performance will impact its final-year performance.
- The annual performance review will include the Supplier's yearly performance, contract spend, and relationship management.

PENALTY FORM: P/001

Details:

Please note that you have committed the following offence(s):

Nature of penalty:

Accordingly, it is proposed that you be liable to pay R_____ as a penalty, due within the same month in which the penalty occurred.

Therefore, please acknowledge receipt of this notice and ensure that payment of the penalty is made within 2 (two) working days from the date of this notice.

Complainant: Technical Security Solution Member

Date: _____

Recommended

Deputy Director: Protection Services

Date: _____

Approval/Not Approved

Director: Protection Services

Date: _____

Received by the successful service provider on _____ (Date)

Signed for by: _____ (Full name)

_____ (Designation)

_____ (Signature)