Specification for a Global Safety & Security Solution (GSSS)
Version 25.1 – March 2025

Contents

1. General Requirements

1.1 Purpose

This document outlines the functional, performance, and implementation requirements for a Global Safety & Security Solution (GSSS). Our organization is seeking a Software-as-a-Service (SaaS) solution that enables seamless communication and coordination among all stakeholders during safety or security incidents.

The ideal solution should be a powerful yet user-friendly command and control system that enhances the Security and Emergency Management Teams' ability to assess and respond to situations in real-time. It should allow staff, customers, visitors, and contractors to quickly request assistance using their smartphones or wearable devices. Additionally, it must ensure proactive safety management, both during and outside working hours, even in isolated circumstances.

We are looking for a comprehensive platform that integrates all aspects of people safety, security, wellbeing, and incident management into a single system. This will help us improve operational efficiency and reduce response times in emergencies.

1.2 Scope

This specification defines the requirements for a cloud-based Software-as-a-Service (SaaS) solution that provides comprehensive security features including: Personal Safety; Mass Communications; Tactical Communications; Wellbeing Support; Tip / Incident Reporting; Travel Safety; First Responder Coordination / Management and Vehicle Tracking.

1.3 System Overview

The GSSS shall provide operators of the system increased situational awareness and efficiency through an integrated command control interface, replacing the need for multi-product single operating interfaces. The GSSS shall provide, either directly as a native feature or through a seamless integration, for control and monitoring of multiple physical security and safety systems such as GPS Tracking, Lone Worker, Mass Communications, Incident Management, Tip Reporting, Wellbeing support and other systems into an easy-to-use single operator interface (Web client or mobile device view).

1.4 Architecture

The GSSS shall be a cloud-based service that supports access securely via dedicated mobile applications and up to date web browsers on workstations, laptops and mobile devices, thus eliminating the need to install, upgrade or support client and server applications software.

The GSSS architecture shall support an app for both iOS and Android Smartphone devices at a minimum for general users.

The GSSS shall also support a mobile app on both iOS and Android Smartphone devices which provides situational awareness and response for the safety Responders.

The architecture must also support a desktop version of the application, preferably deployable as an MSI (Windows Installer file) that can be administered by a corporate IT Services department.

1.5 Compliance & Standards

The system shall comply with the following standards:

- **ISO 27001** for Information Security Management Systems (ISMS)
- **SOC 2 Type II** for security, availability, and confidentiality
- **GDPR or equivalent act** for data privacy and protection
- **WCAG 2.2 AA** for accessibility of the system for end users

---

2. Functional Requirements

2.1 Centralised Management Platform for the GSSS

- The GSSS shall include a single, centralised management platform, “The GSSS portal”, accessible from a COTS browser (e.g. Google Chrome, Edge, Firefox, Safari, etc.)
- The GSSS portal shall have the following key functions:
    - View locations of and manage personal safety alerts
    - View locations of and manage first responders in the field
    - View locations of other users with location sharing enabled
    - View locations of buses / other vehicles on the GSSS system
    - Create and Send emergency mass communications
    - Create and Send geo-targeted and tactical communications
    - Create dynamic chat groups
    - View locations of and manage tip reports
    - Manage Wellbeing support
    - Run reports on historical events from the GSSS
    - Administer and configure the GSSS
- The GSSS shall incorporate a Role-based Access Control (RBAC) approach to limit visibility of the above functions depending on the requirements of the organization and roles of its members.
- Support the specific functional requirements for the GSSS listed in the sections below.

2.2 Personal Safety

2.2.1 Application Alert Functional Requirements

- Users shall be able to raise an alert with a single press of a button within the application
- Alert button shall have a countdown to allow user to cancel alert to before sending to prevent false alerts
- Users shall be able to set the application in a pre-alert state where
    - The user can define a time they want the alert to be raised should they not cancel the timer.
    - The user can enable a fall detection setting which will interrupt the pre-alert state and raise an alert immediately if a fall is detected
    - The user can set a note on the pre-alert to provide additional information to response teams should they not be able to communicate themselves.

    - The pre-alert state, once set, does not require connectivity to escalate to a full alert in the event that, when the timer expires, users phone is for example: out of signal; switched off; otherwise damaged.
- User shall be able to select different alert types based on their situation (minimum 3)
- Raising an alert shall immediately
    - Trigger an alert in a control room
    - Trigger an alert with users of a responder's application
    - Share the user's live location with response teams (mobile and control room based)
    - Share the user's profile information with response teams (mobile and control room based)
    - Open either voice or text-based communication channels
- The user shall be able to see the current state of the alert (Sent, Acknowledged by response team, Cancelled (by themselves), Resolved by Response team)
- Error messages shall be visible to the user raising an alert if it is not able to be sent
- The application should use multiple communications channels to try to sent the alert including
    - WiFi
    - 4G / 5G Data
    - SMS fallback in the event of no cellular or WiFi coverage
- The specific response teams, alerted shall be customizable based on the geographic location of the user when they raise the alert.
- A call button should be available to allow the user to call an appropriate resource based on their location and user profile.
- A messaging button should be available to allow the user to send text-based messages or pictures to response teams
- Raising alerts shall be able to additionally trigger SMS, Email or Push Notifications to the user's supervisor
- Alerts raised outside a Geofence defined by the organization shall prompt the user to call the local emergency services, with the correct phone number, wherever they are located in the World (e.g. 911 USA, 999 UK, 000 Australia, 112 EU, etc.)
- Where alerts are raised outside a Geofence and the user calls emergency services through the application, the response teams shall optionally be able to see an alert icon on a map showing a call to emergency services has been initiated

2.2.2 Paired Device Alert Functional Requirements

- Users shall be able to use a Bluetooth device, paired to the application, to raise alerts
- The device shall have a fall detection which can be optionally enabled by the user when the device is in pre-alert mode
- The device shall have suitable wearable options (e.g. lanyard mount)
- The device shall share battery levels with the application so that alerts can be raised when it falls below a specified threshold
- The device shall signal the user if it loses connection to the phone running the application
- The device shall automatically re-pair to the phone running the application when it comes back into range.

2.2.3 Standalone Mobile Device Alert Functional Requirements

- The solution shall have a range of standalone mobile devices which do not need the application to send alerts to the GSSS.
- The solution shall support a range of devices which are available to support:
    - Standalone satellite communications device
        - for use where there is no Wi-Fi or cellular availability
        - including a pre-alert timer mode
        - including the ability to share location
        - including the ability to receive alert status messages
        - including the ability to receive ad hoc comms from the GSSS
    - Standalone ATEX rated devices for extremely hazardous environments (explosive atmospheres)
    - Standalone cellular devices which shall have as configurable options
        - Automatic call and / or text to a defined number upon alert activation
        - Automatic acceptance of calls from a defined list of numbers (“listen in mode”)
        - An orientation detection alert (if it is detected as being horizontal instead of vertical and vice versa)
        - A no movement detection alert
        - A low battery alert
    - Simple alert devices which
        - operate indoors, independently from a mobile phone
        - report alerts at less than a 10m accuracy on a particular floor of a building (with suitable infrastructure in place).
        - Have a visible low battery display
        - Have a test mode to verify operation
- All devices shall be able to be allocated to and removed from users in the GSSS through a web-portal.

2.2.4 Laptop / Desktop Alert Functional Requirements

- Users shall be able to raise alerts from a Windows computer via an application
- Users shall be able to set their computer’s location within the application including the floor number and room name / number
- The application shall have a single-press emergency duress button which
    - Has a countdown allowing the user to cancel if inadvertently set
    - Shares all currently set location information once sent
    - Shares all profile information of the signed-in user
- The application shall have a pre-alert timer which can be set to alert, if not interrupted, in a defined number of minutes or at a defined time of day
- The application shall show the current alert state (sent, cancelled, acknowledged, resolved)

2.2.5 Response Team Alert Management Functional Requirements

2.2.5.1 Control Room / Dispatch Alert Response

- Control Room Operators / Dispatchers shall have access to the GSSS via web portal through a supported browser for full situational awareness
- GSSS portal shall display alerts on both a map and in an alert list

- Alerts shall be accompanied by an alarm sound which continues until acknowledged by an operator or mobile responder.
- Unacknowledged alerts shall be able to be escalated to other response teams if no response from the primary team is received in an acceptable amount of time.
- Alert icon on the map shall update real-time if the user raising the alert moves
- Map shall support different views including geographic markers and satellite view, Google layers for labels of points of interest (e.g. roads, shops, restaurants, parks, etc.)
- Map shall support custom overlays (for example showing defibrillators) via image import or a geographic marker file (e.g. GeoJSON, KML, etc.)
- An alert card shall show key information to the responders at a glance including
    - Name
    - Alert Type
    - Alert State
    - Last updated timestamps for location and communications
    - Alert triggers (if present) including
        - Fall detection
        - Crash detection
        - Low battery
        - Disconnection
- Expanding the alert card shall provide more detailed information on the user including
    - All user profile information
    - User Group membership including details of any supervisors
    - Location (GPS, UTM, MGRS, and nearby addresses)
    - Building floor (where indoor positioning available)
- In the expanded alert card, operators shall be able to
    - Change the alert state
    - Add resolution notes
    - Chat with the Alert Raiser and other mobile responding officers.
- GSSS portal shall automatically display the corresponding floor plan when an alert is raised in a building with indoor positioning integrated to the GSSS
- GSSS Portal shall show available mobile responders on the map including, floor-level accuracy for responders in a building with indoor positioning integrated to the GSSS
- GSSS Portal shall allow operators the ability to communicate with groups of responders via text-chat in response to an incident in addition to the ability to use text chat to communicate with the alert raiser.
- Upon resolving an incident, the GSSS shall
    - Allow the operator to select an appropriate closing category
    - Allow the operator to add notes to the incident
    - Store the alert for later review including
        - Alert Type
        - Date / Timestamps
        - Responder actions
        - Text-based chat exchanged between responders and the alert raiser
        - Playback video, including timestamps, showing the movements of the alerts and all responding officers on a map

2.2.5.2 Mobile first responders Alert Response

- Mobile first responders shall be able to visualise any alerts and the live locations of their colleagues, via a mobile responder application, giving them full situational awareness
- The mobile responder app shall display alerts on both a map and in an alert list
- Alerts shall be accompanied by an alert sound.
- Map shall support different views including geographic markers and satellite view.
- Alert icon on the map shall update real-time if the user raising the alert moves
- Pressing the alert icon will give the responder access to key information to the responders at a glance including
    - Name
    - Alert Type
    - Alert State
    - Last updated timestamps for location and communications
    - All user profile information
    - Building floor (where indoor positioning available)
- Mobile responders shall be able to interact with the alert on screen:
    - Changing the alert state (acknowledging or resolving)
    - Adding resolution notes
    - Chat with the Alert Raiser and other mobile responding officers.
    - Call the Alert Raiser
- The mobile application should automatically display the corresponding floor plan when an alert is raised in a building with indoor positioning integrated to the GSSS
- The mobile responder application shall give operators the ability to communicate with groups of responders via text-chat in response to an incident.
- The mobile responder application shall include a duress button in that the first responders themselves require immediate assistance.

2.3 User location sharing

- All users in of the GSSS shall be able to share their location through a safety application.
- Location sharing shall be opt-in and users shall be able to control when they are visible
- Users shall be able to escalate their location sharing into a pre-alert state where timers, notes and fall detection can be enabled for their safety
- Location sharing shall cease when users exit the organization's geofences unless that location sharing is due to
    - An alert being raised
    - The user being in a pre-alert state.
- Location sharing shall be able to start automatically when the user enters a geofence
- Upon entering a geofence with location sharing enabled, users shall be able to receive push notifications pertinent to that area, the time they access the area and their own group membership.
- Users shall be able to be prompted to start sharing their location in an emergency via push notification from the GSSS.
- Location sharing for certain, high risk groups shall be able to be escalated into an alert if the session ends prematurely (i.e. is not naturally ended by the user due to battery failure, device being damaged, etc.)
- User location sharing shall be only provided to authorized users in the GSSS.

- User authorization to view those sharing locations shall be granular so that a supervisor could see their own team's locations but not that of other teams.

2.4 Mass Communications

- The GSSS shall incorporate mass communications across at least the following channels:
    - Push Notifications to safety and mobile responder applications
    - SMS (whether users have the applications or not)
    - Email
    - Desktop takeover
    - Satellite devices communications
    - Voice calling
    - Web feed publishing (for integration with other apps, digital signs, or websites)
    - Other standalone alert devices which have displays (as described in the Standalone Mobile Device Alert Functional Requirements section)
- Templates shall be able to be created with pre-populated content to allow quick sending of vital messages to a large audience
- Templates shall be able to have pre-populated target groups setup
- Templates shall be able to include drop-list selection tools for content customization within pre-approved parameters
- Templates shall be able to be limited so that only certain authorized users can send them based on
    - Category of notification
    - Recipient Groups
    - Channels used
- Users shall be authorized to either only send templated messages or to edit the message content before sending
- Privileged users shall be able to send fully customized messages ad hoc as required
- Templates shall be disabled as default until approved by an authorized person
- Dynamic templates shall be able to be created which will be targeted based on criteria defined in a GSSS workflow and not a fixed user list (e.g. send a message to a triggering user when they raise an alert)

2.4.1 Push Notifications

- Push Notifications sent from the GSSS shall be able to be targeted based on user group membership
- Push Notifications shall be able to be targeted based on a recipients live location (without the need for them to be in location sharing mode)
- Location-based targeting should utilise search tools such as Google to fly to appropriate areas of the map and defined further through a drawn shape on screen.
- Push Notifications shall be able to be targeted at only responder app users, only safety app users, or both app types
- Push Notifications shall include options on how they are delivered including with an alarm sound, default notification sound, silent with vibrate, silent only.

- Importantly for the above delivery settings, these should NOT override the phone's own settings to avoid giving user locations away in an active threat scenario.
- Push notifications shall include the ability to send a location sharing request to the recipient
- Push notifications shall be able to include a web-link to an external site for further information
- Push notifications shall include an option title in addition to the message body

2.4.2 SMS Notifications

- SMS Notifications sent from the SMS shall be able to go to all users in the system or only users who have not got the safety application (if deduplication is required)
- SMS data shall be able to be pre-loaded into the GSSS by the organization
- Organizations shall be able to create self-signup campaigns for visitors to temporarily receive notifications for a defined duration
- Self-signup campaigns shall have different durations configured for how long visitors are subscribed (e.g. 1 day; 1 week; 12 weeks; etc)
- Self-signup campaigns shall be able to be specifically targeted by comms (i.e. ability to send messages to visitors for an event, but not those signed up through a contractor registration campaign)
- SMS shall be compliant with legislation around user opt out

2.4.3 Email Notifications

- Email notifications shall be able to be sent including a message subject and body
- The email body should support rich text formatting
- The email channel shall be able to be integrated with the organization's DNS settings so that the originator appears to be from within the organization
- Emails shall have configurable header content for the email body (e.g. to include organizational logos.
- Emails shall have configurable footers (including the optional management or notification preferences)

2.4.4 Desktop Takeover

- GSSS shall be able to send messages to laptops and desktops managed by the organization
- The screen takeover software shall work on both Windows and Mac machines
- The screen takeover software shall be able to work even if Windows machines are logged off
- The screen takeover software shall be able to target groups of machines based on network settings, computer name systems, or manually allocated to groups.
- The screen takeover software shall have text to speak capabilities
- The screen takeover software shall be able to override computer volume settings
- The screen takeover software shall support different profiles to suit the message, including
    - Full-screen takeover
    - Partial screen pop-up (configurable size and location on screen)
    - Rolling scroll bar (configurable size and location on screen)
- Screen takeover profiles shall support organizational logos and colour palettes.

2.4.5 Satellite Notifications

- The GSSS shall support the sending of emergency communications to defined satellite devices (e.g. Garmin InReach). This will allow communications to continue with key resources when other power and communications infrastructure is degraded.

2.4.6 Voice Calls

- The GSSS shall be able to send voice calls to defined devices which read allowed in suitable text to speech format.
- The voice messages shall be able to repeat at least twice
- The voice message shall be able to leave a voicemail if the user is unavailable
- The voice calls should be high-bandwidth and capable of quickly calling thousands of users.

2.4.7 Web feed publication

- Web feeds shall be able to be published through the GSSS
- Web feeds shall support the following formats
    - JSON
    - XML
    - RSS
    - EDXL (Common Alert Protocol – CAP)
- Web feeds shall be published to a defined URL to be polled by 3rd party systems
- Web feed documents shall have optional expiry dates applied

2.4.8 Communications with other devices

- The GSSS should also support communications to other standalone devices, which are used for personal safety, and have appropriate screens to display messages

2.4.9 Mass Communications Integration Options

- The GSSS shall have an API available to allow 3rd party systems to poll events and send notifications through other channels
- The GSSS shall be able to accept notification send requests that are sent from 3rd party systems which are sent in a compatible REST API format
- The GSSS shall have off the shelf integration to 3rd party channels through the publishing of a web feed in Common Alert Protocol (CAP) format.
- The GSSS shall be able to poll events from 3rd party sources and automatically incorporate them into mass communications via it's own channels (for example to republish a FEMA event to its user base in the GSSS):
    - EDXL
    - ATOM CAPS
    - ATOM GEO RSS
    - GEO RSS
    - FEMA IPAWS (CAPS)

2.5 Incident Management and Tactical Communications

- The GSSS shall visualise on a live map all resources available in the event of an incident

- The GSSS shall be able to filter the map view to only view specific resources or groups of users
- The GSSS shall include a map capture tool to lasso resources on a map and either
    - Send a 1-way targeted notification to them
      or
    - Add them to an encrypted chat group
- The map capture tool shall also be able to lasso multiple personal safety alert triggers (e.g. in a mass casualty incident) and send a message to all alert raisers in one action.
- The GSSS shall support customized map layers which can show important fixed resources, features or risks on the map, including
    - Defibrillators
    - Stop the bleed kits
    - Narcan kits
    - Hazardous materials
    - CCTV cameras
- Icons on the customized map layer shall be in png format or similar, include a title and a description (which can itself include a clickable URL to link to further information or video feeds)

2.6 Wellbeing Support

- The GSSS shall also have a tools to support the wellbeing of all application users.
- The wellbeing support shall include a button which provides the user contextual support based on
    - Who they are
    - Where they are located
    - The time they interact with the tool (based on organization-defined schedules)
- Support options shall include
    - Links to websites
    - Call to a defined number
    - SMS to a designated number
    - Email to a nominated mailbox
    - Opening a text-based chat with the organization's mental health trained responders who will reply via either the application or the GSSS web portal
- The schedule for the wellbeing tool shall accommodate special events / holidays and be able to be programmed in advance.

2.7 Tip Reporting

- The GSSS shall accept tip reports sent from the safety application
- The reports shall be able to be sent either named or anonymously
- The reports shall be able to be sent with or without a location
- The reports shall be able to be sent with or without an image

- The organization shall be able to define categories of tip report with different settings including
    - Category title
    - Category guidance
    - Customized acknowledgement message to each category
    - The ability to remove the anonymity option to a specific category (/ categories)
    - The ability to restrict visibility to that category for some GSSS operators
    - The ability to forward tips from a specific category to a defined recipient list via email

2.8 API & Integration

2.8.1 General Integration Requirements

- The GSSS shall be a platform which can be integrated to 3rd party systems via API
- The GSSS shall also offer off the shelf integration for industry standard protocols such as SAML 2.0 and Common Alert Protocol
- The GSSS shall have an open architecture which does not limit integration with 3rd party systems

2.8.2 Alert Integration

- The GSSS shall accept alerts from 3rd party sources / systems which are sent via REST API.
- The alert data from the 3rd party shall be sent via API to the GSSS Cloud server and include at least:
    - GPS location
    - Alert type
    - Floor level (of building if applicable)
    - A suitably authenticated account
- Example alerts received into the GSSS may include: exception events from CCTV systems, Access Control Systems, Fire Systems, other Building alarm Systems
- The GSSS shall make available a list of alerts raised within the system for access by 3rd party incident management platforms
- The Alert data shall be accessible via polling from an authenticated account and be able to retrieve all relevant information (Name, email address, alert state timestamps, alert type, GPS coordinates, Floor level, Resolution Category, etc)

2.8.3 User Management

- The GSSS shall be able to integrate user data via REST API and have calls available for all CRUD functions
- The GSSS shall support SCIM as a data source for user data management and user group population

2.8.4 Indoor Positioning

- The GSSS shall be able to integrate with existing Indoor Positioning Solutions including from tech companies such as Cisco, Juniper and HPE Aruba
- The GSSS shall have its own indoor positioning solution available, independent of the organizations own network, for scenarios when an integration with an existing provider is not practicable

2.8.5 Alliance

- The GSSS shall be able to be linked with similar systems around the World so that
    - If an end user visits another GSSS user while working away, they will be able to activate a duress alert and get support by that organization.
    - If a visitor to the organization's site also has a compatible GSSS from their organization, they will be able to get support while on our premises through the same application
- For the above scenarios, both end users and organizations must opt in for privacy purposes

---

3. Performance & Scalability

3.1 High Availability

- The GSSS is a life-safety system and, as such shall have a minimum 99.9% uptime
- Infrastructure and all data within shall be geo-redundant failover meaning that there is a backup copy in another region should an entire datacentre fail
- Disaster Recovery (DR) plan with RPO ≤ 4 hours and RTO ≤ 8 hours
- Load balancing with auto-scaling capabilities
- All updates shall be deployed without interruption to service levels allowing zero downtime
-

3.2 Scalability

- The platform should be deployed on a cloud infrastructure (e.g., AWS, Azure, Google Cloud) that supports auto-scaling.
- Dynamic resource allocation based on workload demand

---

4. Security & Privacy Controls

4.1 Security Controls

- All data in the GSSS shall be encrypted both at rest and in transit
- GSSS shall use TLS 3.0 to secure all communications over the internet
- Web Application Firewalls (WAF) shall be in place with a stateful packet inspection (SPI) firewall
- The GSSS supplier shall implement next-generation persistent threat (NGPT) monitoring
- The GSSS shall have a 24x7x365 monitoring system to counter intrusions
- Penetration Testing shall be conducted at least annually by the GSSS supplier

4.2 Authentication & Authorization

- The GSSS shall have a comprehensive Role-Based Access Control (RBAC) system in place to segment permissions and allow data minimization.
- The database shall restrict IP access to the internal application servers only (no external web access) and access must be restricted to internal credentials.
- The GSSS shall provide application server components that support a non-authenticated entry point and an authenticated entry point. The non-authenticated entry point (anonymous) provides access to functions such as self-registering to the system the end user App. Non-authenticated access is extremely restricted.
- The solution shall utilise authenticated entry point to authenticate a user immediately by using the Secure Challenge Response Authentication Mechanism (SCRAM). SCRAM uses nonces and hashes to challenge the authenticating party to provide a token to verify their identity.
- The solution shall support SAML 2.0 integration for identity authentication (variants such as Entra (Azure AD), ADFS, Open Athens, Shibboleth, and google as examples)

4.3 Data Residency & Privacy

- The system shall be able to be deployed in an appropriate regional database center to comply with local laws and regulations.
- Pseudonymization and anonymization of personal data shall be in place whenever practicable
- Configurable data purging options shall be available based on the data type in use, specifically the organization shall need to specify how many days the following data is stored:
    - Alert data
    - Notification Data
    - Location Sharing Data
    - (Soft) Deleted User data
    - First Responder Management Data
    - Chat Data
    - Tip Report Data

5. Deployment & Management

5.1 Deployment Requirements

- Fully managed SaaS deployment with logically separated databases to partition data
- Project implementation plan developed in partnership with the Customer Success Manager
- Phased approach to implementation to match organizations goals

---

6. Reporting & Analytics

6.1 Alert History Reports

- GSSS shall be able to run reports on alert history as far back as the data retention period is configured.
- A recent alerts page shall be available in the GSSS showing the last 3-days of events
- Each item on the recent alerts page will display information in the following columns:
    - **Raised** - the date and time when the alert was raised by the end-user;
    - **Last Updated** - the date and time when the last update occurred on the alert;
    - **Alert icon** - showing which type of alert was raised on the SafeZone app;
    - **Raiser** - the SafeZone user who raised the alert;
    - **Details** - clicking on **Details** brings up the History of the alert.
    - **Restore** - clicking on **Restore** allows you to restore the alert. This is useful if the alert was resolved in GSSS by an operator but the alert/incident is still taking place. The alert will re-appear on the Live screen as an alert which the GSSS operators and Mobile First Responders can respond to.
- The GSSS shall also have a general alert reporting history which shall allow an authorized user to search for alerts raised in the GSSS and apply filters including:
    - Region
    - Region Group
    - Date and Time Range
    - Alert Type (e.g. First Aid, Emergency, Check-in, Test, etc...)
    - Resolution Category
    - User
    - User Group
- The alert history report generated from the above shall include a table with at least the following columns:
    - **Raised** - Date and time the alert was raised (NOTE this is according to your local time per your computer settings)
    - **Last Updated** - When the alert last had interaction (e.g. Resolution, Cancellation, Restoration)
    - **Alert Type Icon** - showing the type of alert raised (Duress, First Aid, Help, Check-in, First Aid, Police Call, Ambulance Call)
    - **Raiser** - the user who raised the alert and their phone number
    - **Details** button - takes you to a screen with more information on the alert and a geographical playback

- The alert playback shall display all movements of the alert raiser, in addition to responders on a dynamic, timestamped map.
- The alert playback shall be able to trace the alert path as it moves along the map.
- The alert history reports shall be exportable with key information including
    - Raiser Name
    - Raiser Email Address
    - Alert Type
    - State (e.g. Acknowledged, Resolved, Cancelled)
    - Resolver Name
    - Resolver Email Address
    - Whether the alert was a "Test Alert"
    - Last Updated Timestamp
    - Raised Timestamp
    - Acknowledged Timestamp
    - Cancelled Timestamp
    - Resolved Timestamp
    - Resolution Category
    - GPS coordinates of the alert when raised
    - Floor level (If indoor positioning is present)

6.2 Location Sharing Data Reports

- The GSSS shall be able to run reports of users who have shared their location through the safety application
- The reports shall be able to be filtered by
    - Date
    - Time
    - Region
    - Floor Level (if present)
    - User
    - User Group
- The reports shall be exportable in a machine-readable format
- The GSSS shall also be able to generate heatmap reports of the location sharing events

6.3 First Responder History Reports

- The GSSS shall be able to run a playback on historical movements of users with the Mobile Responder Application
- The playback reports shall be able to be filtered by
    - Date
    - Time
    - Region
    - Region Group
    - User
    - User Group
- The GSSS shall also be able to generate heatmap reports of the Mobile Responders' patrols while using the application

6.4 Tip History Reports

- The GSSS shall report on all Tips received by the system
- Tip History Reports shall have the following filters available
    - Date and time
    - Tip Status (open / closed)
    - Tip Category
- Tips shall be able to be exported in a machine readable format with at least the following columns:
    - Status
    - Date/Time
    - Category
    - Resolution Date/Time
    - Resolver
    - Resolution Notes
    - Raiser Given Name
    - Raiser Last Name
    - Raiser Email
    - Link (to the original tip in GSSS)
- A tip detail screen shall show further information on a specific tip including:
    - When the tip was raised, its status and category
    - The tip raiser's information (if not submitted anonymously where < Anonymous > should be displayed
    - A map of the location (if submitted without a location "No location information given" will be written across the screen)
    - Messages section where the tip notes and any submitted images will be displayed

6.5 Mass Communication History Reports

- The GSSS shall include detailed reports on the status of mass and tactical communications sent from the system
- The GSSS shall allow the exporting of a summary list of previous activations in a defined time frame
- The summary list report shall include at least:
    - Timestamps
    - Sender name
    - Recipients (User Group level)
    - A summary of the message content and channels used
- Individual reports on a specific notification shall be available which shall at least include:
    - The sender and time the notification was sent
    - Which notification group(s) it was sent to
    - The delivery method(s) for the notification and the progress of each method.
- For SMS messages enhanced reporting shall be available showing delivery status which follows standard international SMPP protocols.

---

7. Support & Maintenance

7.1 Technical Support

- 24/7 customer support through multiple channels including, telephone, email, in-application, in-portal
- Dedicated Customer Success Managers allocated to the organization
- In-product User Guides
- Online Training Academy
- Online status page which allows the organization to subscribe to any system issues via at least:
    - SMS
    - Email
    - RSS Feed
    - Atom Feed
    - Webhook
- In-person train the trainer options

7.2 Software Updates

- GSSS updates shall follow a defined change management process
- GSSS development shall follow an agile framework with regular (monthly) security patches and feature updates
- Zero-downtime deployment for updates
- Backward compatibility assurance for API changes