

Symphia NowForce A&E

Version 6.1

June 2023

Unauthorized use, duplication, or modification of this document in whole or in part without the written consent Intellicene Inc. is strictly prohibited. By providing this document, Intellicene Inc. is not making any representations regarding the correctness or completeness of its contents and reserves the right to alter this document at any time without notice. Features listed in this document are subject to change. Contact your Intellicene representative for current product features and specifications. All marks referenced herein with the ® or TM symbol are registered trademark or trademarks of Intellicene Inc. or its subsidiaries. All rights reserved. All other marks are trademarks of their respective owners.

© 2023 Intellicene Inc. All Rights Reserved Worldwide.

#### Table of Contents

[Solution Architecture 3](#_Toc138080874)

[Security 4](#_Toc138080875)

[System Integrations/ APIs 5](#_Toc138080876)

[System Server Components 6](#_Toc138080877)

[System Client Components 7](#_Toc138080878)

[Localization 8](#_Toc138080879)

[Admin/ Settings System Configuration 9](#_Toc138080880)

[User Management 9](#_Toc138080881)

[License Management 10](#_Toc138080882)

[User Permission Profiles 10](#_Toc138080883)

[Applicant/User Registration/Enrollment Management 10](#_Toc138080884)

[User Policies 11](#_Toc138080885)

[User Updates Settings 11](#_Toc138080886)

[Groups Configuration 12](#_Toc138080887)

[Roles Configuration 12](#_Toc138080888)

[Equipment Configuration 13](#_Toc138080889)

[Units Settings 13](#_Toc138080890)

[Multiple Control-Center/Agency Configuration 14](#_Toc138080891)

[Branding – Icons & Logos 15](#_Toc138080892)

[SMS/Email Configuration 15](#_Toc138080893)

[Maps/GIS Settings 17](#_Toc138080894)

[GIS Map Configuration 17](#_Toc138080895)

[GIS POI Configuration 17](#_Toc138080896)

[GIS Polygon/Geofence Configuration 17](#_Toc138080897)

[Incident Management Settings 19](#_Toc138080898)

[Incident Configuration 19](#_Toc138080899)

[Auto Dispatch Rule Configuration 19](#_Toc138080900)

[Dynamic Forms for Incidents 20](#_Toc138080901)

[Incident Dynamic Situation Reports Configuration 22](#_Toc138080902)

[Dispatcher/Operator Desktop Application 23](#_Toc138080903)

[General UI Guidelines 23](#_Toc138080904)

[Login & Access Control Security 23](#_Toc138080905)

[Users Panel/Grid 23](#_Toc138080906)

[Operations (Incidents) Panel/Grid 24](#_Toc138080907)

[Operational Map & Geofencing Management 24](#_Toc138080908)

[Resources Monitor 25](#_Toc138080909)

[Alerts & Notifications 25](#_Toc138080910)

[Incident Creation/Call Taking 26](#_Toc138080911)

[Dispatching 28](#_Toc138080912)

[Incident Management & Progress Gauge 28](#_Toc138080913)

[Other Dispatch Tools 29](#_Toc138080914)

[Assets - Incident Intelligence 29](#_Toc138080915)

[Forms - Incident Data Collection 30](#_Toc138080916)

[Incident Log and Data Summary 30](#_Toc138080917)

[Scenario/Event Planning 30](#_Toc138080918)

[Smart Messaging 31](#_Toc138080919)

[Mobile Application 32](#_Toc138080920)

[Mobile Application Modularity and Basic Functionality 32](#_Toc138080921)

[Mobile Status, Locations and Communication Check 33](#_Toc138080922)

[Mobile SOS 34](#_Toc138080923)

[Mobile Reporter 35](#_Toc138080924)

[Mobile Responder 36](#_Toc138080925)

[Mobile Supervisor 37](#_Toc138080926)

[Mobile Messaging 38](#_Toc138080927)

[Mobile Asset Lookup 38](#_Toc138080928)

[PTT 38](#_Toc138080929)

[Escort Me 39](#_Toc138080930)

# Solution Architecture

1. The system shall have a flexible, open platform architecture built on accepted industry standards that facilitate integration with IT infrastructures.
2. The system shall support running on COTS (commercial off the shelf) computer server.
3. The system shall be able to be installed in a Virtual Environment (e.g. Vmware).
4. The system shall be able to be installed both on a cloud-based environment (eg. AWS, MS Azure) and on-premise
5. The system shall be able to be support both single-tenant and multi-tenant architecture allowing multiple organizations to run on one DB environment.
6. The solution will provide an option for redundancy, using separate servers, and achieve a fault tolerant, zero downtime environment.
7. The solution shall be redundant, using two separate servers, and achieve a high availability, minimal downtime environment. This design should not result in any data loss, however may require manual or automatic start of the application on the secondary server.
8. The solution shall provide a disaster recovery option, using a third separate server at a secondary location which would assume primary responsibility in the event of a catastrophic event at the primary location.
9. The system Server component shall support software designed for the Microsoft Windows 2016 R2 (64 bit).
10. The system Client component shall support Microsoft Windows 7, or Windows 8 or Windows 10 (32 or 64 bit) operating systems for workstations.
11. The system shall be localization-ready and include support for Unicode characters, including double-byte and extended characters.
12. The vendor should be ISO 9001 certified.

# Security

1. The Encryption
   1. The system’s web interface shall use SSL/TLS encryption.
   2. The system’s mobile applications shall use SSL/TLS encryption.
   3. The system shall assign a unique ID to each connected mobile device.
   4. The system shall allow the option to limit the access to its web interface to specific IP ranges.
2. Login & Password Security
   1. The system shall support a single device login (to prevent multiple logins from the same account).
   2. The system shall support enforcing a login verification process with a code sent via SMS and/or email (“Two-factor authentication”).
   3. The system shall support limiting idle sessions on the browser by time intervals (forced log-out for sessions with no activity).
   4. The system shall have all passwords stored in the database hashed.
   5. The system shall support a policy to enforce password expiration/renewal.
   6. The system shall support strong password enforcement.
3. Certification
   * The system’s infrastructure shall support ISO 27001.

# System Integrations/ APIs

1. The system shall be an open architecture system allowing simple integration to external modules, sensors and systems, and allowing future scalability.
2. The system shall be vendor agnostic and have the ability to interface with variety of systems and devices including:
   1. Panic button systems
   2. GPS tracking (AVL) systems
   3. CAD/CRM/PSIM systems
   4. C4I systems
3. The system’s API will support the integration of a new device/system via RESTfull WebServices (XML, JSON).
4. The system’s API will support the integration of a new device/system via TCP/IP.
5. The system’s API will support the integration of a new device/system via EMAIL.
6. The system’s API will support the integration of a new device/system via SMS.
7. The system’s API will support inbound and outbound actions.
8. The system’s API will support definition of parameters via regular expression.
9. The system’s API will support definition of parameters via delimited values.
10. The system’s API will support search/replace functionality for address verification.
11. Configuration of a new inbound device via the supported protocols and methods shall not require a core product release, configuration shall be done using the user interface or database/application configuration.
12. The API will provide the ability to post a new incident to the system.
13. The API will provide the ability to auto dispatch users to an incident (based on the pre-defined dispatch rules).
14. The API will provide the ability to dispatch specific users to an incident.
15. The API will provide the ability to post incident statuses.
16. The API will provide the ability to create a new user.
17. The API will provide the ability to retrieve basic user details and statuses.
18. The API will provide the ability to post a user location to the system.
19. The API will provide the ability to query the system for basic incident details and statuses.
20. The API will provide the ability to query the system for user locations.

# System Server Components

For details on on-prem server/IT requirements, refer to CFE/VSE documentation.

# System Client Components

1. The system’s Client (Operator/Dispatcher) workstation shall be able to support the following configuration:
   1. Computer with at least 2GB of RAM and 10GB of available storage space.
   2. Operating System - Windows 8 or 10 with latest updates/service packs.
   3. Web Browser (Chrome) with latest updates/service packs.
   4. Monitor(s) - high resolution display (1024X768 or above).
   5. Keyboard + Mouse + Speakers (for audio alerts).
   6. High speed internet connectivity (in case where a local server is used, a high speed LAN/WAN connection is required).
2. The mobile devices running the system’s application shall be able to support the following devices:
   1. Android (OS version 6 and higher) with Google API or Static IP address.
   2. iPhone (iOS version 10.0 and higher).
   3. Web-based app for SOS and Reporter features.

# Localization

1. The system shall support localization of the end-user’s device (desktop and mobile) to multiple languages.
2. The system shall support the following languages:
   1. Arabic
   2. English
   3. German
   4. Hebrew
   5. Italian
   6. Japanese
   7. Portuguese
   8. Russian
   9. Spanish
   10. Ukrainian
   11. Vietnamese
3. The system shall support localization to multiple time zones.
4. The system shall support localization to metric/imperial formats.
5. The system shall support multiple date formats.

# Admin/ Settings System Configuration

## User Management

1. The system shall allow creation of users via graphic user interface.
2. The system shall allow bulk upload of users via Google Spreadsheet with field validation rules to maximize data integrity when uploading the data.
3. The system shall allow adding basic user details such as name, alias, phone numbers, email addresses, home/work addresses.
4. The system shall allow creation of username and password for each user.
5. The system shall allow attributing users with one or more Group.
6. The system shall allow attributing users with one or more Role.
7. The system shall allow attributing users with one or more Equipment Type.
8. The system shall allow attributing users with geographical assigned areas (geofence / polygon / territory / jurisdiction).
9. The system shall allow attributing users with associated control centers/agencies.
10. The system shall allow attributing users with a distress call phone number.
11. The system shall allow enabling and disabling specific users.
12. The system shall allow to assign each user to customized system profiles. The profile will define which system licenses are assigned to the user, thus defining access of user to the modules, features and capabilities of the system.
13. The system shall allow creating multiple permission profiles and associating them to users, thus defining a customized set of permissions and system access for the users.
14. The system shall allow associating one or more emergency contacts to each user. The emergency contacts can also be set in the mobile app.
15. The system shall allow sending a password reset via the user interface by the administrator. The reset password can also be done in the mobile app.
16. The system shall display the list of all or specific users based on multiple attributes and search criteria including searching users based on their current location (within a geofence).
17. The system shall allow to search users with auto-complete mechanism.
18. The system will display user’s current availability status on the system.
19. The system will display user’s current and historic locations and statuses.
20. The system will display user’s current and historic locations including the age of current location both on a map (breadcrumbs/ trail) and in a textual table.
21. The system will display user’s current communication with server status.
22. The system will display user’s current mobility method.
23. The system will display the user’s current load of incidents.
24. The system shall allow filtering the users list by different attributes (e.g. group, role, status, device type etc.)
25. The system shall allow searching for specific users by unique ID, name or other properties.
26. The system shall allow editing and modifying user details via the user interface.
27. The system will allow users to turn on/off (activate/deactivate) attributed roles/equipment.
28. The system shall allow the association of users with geofence/polygon and automatically trigger an alert or activate an incident if a user enters or exits this geofence/polygon.

## License Management

1. The system shall provide the Administrator visibility of available licenses.
2. The system shall provide the Administrator visibility of which system capabilities/features are provided with each license.
3. The system shall provide the Administrator visibility of the expected expiration/renewal date of licenses.
4. The system shall provide the Administrator visibility of licenses that are reaching a limit and require renewal, upgrade or expansion.

## User Permission Profiles

1. The system shall allow the creation of (unlimited) permission profiles.
2. The system shall enable the administrator to define for each permission profile the relevant set of system licenses (desktop and mobile) and define which system capabilities and controls will be available for the users associated with this profile.
3. The system shall display the amount of users associated with each profile.
4. The system shall prevent deleting of permission profiles that are associated with existing users.
5. The system shall present the administrator with all the permissions that are associated with each permission profile.
6. The system shall provide permission based access to different level of information including: user interface access, ability to activate specific features, ability to view and/or search for specific user groups. ability to view and/or manage incidents based on access to agency/center.

## Applicant/User Registration/Enrollment Management

1. The system shall allow the administrator to send users a link to a dedicated registration portal.
2. The system’s registration portal shall be able to display the customer’s logo.
3. The system’s registration portal shall be able to collect the phone number, email address, home address and photo of the user.
4. The system shall be able to send the applicant an SMS to verify integrity of the applicant’s identity.

## User Policies

1. A policy is a set of behaviors/guidelines that are enforced on users using multiple tools in the system: messaging, location tracking, geofencing, access control, dynamic forms, contact tracing etc.
2. The system shall allow the Admin to create and modify multiple Policies for the organization and assign users to policies.
3. Each policy has transition (entrance and exit) rules that can be triggered automatically based on events or information sent by the user.
4. The policy settings include the following tools on the end-user’s end:
   1. Location sampling/saving/sharing parameters
   2. Geofencing triggers (in/out)
   3. Simple mobile tool for users to send situation updates and dynamic forms
   4. Bluetooth and/or location based Contact Tracing (Exposure Notification)
   5. Personal QR codes for Access Control
   6. User personal log that registers and archives all events for each user
   7. Registration web-page
5. The policy settings include the following tools on the supervisor/operator side:
   1. QR code scanning by supervisors
   2. Search/filter tool for retrieving registered events based on various search criteria
   3. Capacity parameters for policies and areas (geofences/facilities)
   4. Operator dashboard displaying real-time allocation of users from the entire workforce in policies and geofences/facilities
   5. Ability to interface with 3rd party access control and imaging/scanning devices

## User Updates Settings

1. The system shall allow the Admin to define dynamic updates that the mobile users can post to the user’s log.
2. The Admin can create multiple types and formats for user updates including the following:
   1. User update name, icon and category.
   2. User update formats can include a simple title update, an update with free text entry and an update with a dynamic form.
   3. Admin can define whether the user update will be sent to the server with or without user’s location.
   4. Admin can define whether posting a user update will trigger an alert in the dispatcher/operator.
   5. Admin can define for each user update events that trigger the user update.
   6. Admin can define for each user update events that will be impacted by the user update.

## Groups Configuration

1. The system shall allow creation of one or more groups.
2. The system shall allow associating each group with a unique ID, name, details and icon.
3. The system shall enable the administrator to associate a group with users either through the user management interface or via the groups management interface.
4. The system shall allow the assignment of groups to control centers (many to many) thus granting group moderators jurisdiction and access to view, manage and perform operational actions on the group members (send messages, dispatch, view on map etc.).
5. The system shall allow the creation of chat and PTT channels for each group.
6. The system shall present for each group the amount of members and of moderators (who have jurisdiction over the group), as well as the name of the group creator and the date of the last modification.
7. The system shall allow each user to be associated with more than one group (many to many).
8. The system shall allow the soft-delete of groups.
9. The system shall prevent deleting groups that are the only group of any single user. In this case an alert will notify there are users that first need to be moved to another group.
10. The system shall allow to define emergency contacts for any group. These contacts can be notified automatically when a member of the group performs an action (i.e. activates SOS alert).
11. The system shall have a group history log displaying modifications performed in the group’s history.

## Roles Configuration

1. The system shall allow the creation of one or more role.
2. The system shall allow associating each role with a unique ID, name and icon.
3. The system shall present for each role the number of associated users.
4. The system shall allow each user to be associated with more than one role.
5. The system shall allow the soft-delete of roles unless they are assigned to existing users.
6. The system shall allow to define required roles to respond to Incidents
7. The system shall allow to define required roles for a unit.
8. The system shall allow to display which roles are currently available in a specific area/geofence.

## Equipment Configuration

1. The system shall allow creation of one or more equipment type.
2. The system shall allow associating each equipment with a unique ID, name and icon.
3. The system shall present for each equipment the amount of associated users.
4. The system shall allow each user to be associated with more than one equipment.
5. The system shall allow the soft-delete of equipment/s unless they are assigned to existing users.
6. The system shall allow to define required equipment types to respond to Incidents
7. The system shall allow to define required equipment types for a unit.
8. The system shall allow to display which equipment types are currently available in a specific area/geofence.

## Units Settings

1. The Unit entity allows to link together multiple users that operate under one unified entity and perform their actions/tasks/incidents as a joint unit (with or without a vehicle).
2. The system shall allow creation of Units via graphic user interface.
3. The system shall allow adding unit details such as operational code, unit name, unit type.
4. The system shall allow to associate users to a unit as unit members.
5. The system shall allow defining for each unit type a set of minimum and maximum required unit members based on their organizational credentials (groups, roles and/or equipment).
6. The system shall display an alert if the combination of roles of members associated with the unit exceeds or falls short of the unit’s requirements.
7. The system shall allow creation of username and password for each unit.
8. The system shall allow attributing units with one or more Equipment.
9. The system shall allow attributing units with one or more geographical area (polygon/ geofence) and alert on entrance/exit of geofence.
10. The system shall allow attributing units to be under jurisdiction of control center/agency.
11. The system shall allow associating a unit with a mobile device or location tracker (AVL etc.) and record the unit’s locations.
12. The system shall allow enabling and disabling specific units.
13. The system shall allow defining for each unit type dedicated statuses.
14. The system shall display the list of all or specific units.
15. The system shall allow to search (with auto-complete mechanism) for any unit. Searching for a unit will display the unit’s details and location on map.
16. The system will display unit’s current and historic locations including the age of current location.
17. The system will display unit’s current communication with server status.
18. The system will display the unit’s current load of incidents.
19. The system will display the unit’s current associated users.
20. The system will display the aggregate roles of users associated with it.
21. The system shall allow searching for specific unit by its unique ID, name or other properties.
22. The system shall allow editing and modifying unit details via the user interface.

## Multiple Control-Center/Agency Configuration

1. The system shall allow the organization to work either as one central command & control center or with multiple control centers that have different levels of jurisdiction and responsibilities.
2. The system shall allow creation of one or more control center/agency.
3. The system shall enable administrators to associate each center/agency with a unique ID, name, and phone number.
4. The system shall enable the administrator to define jurisdiction of control centers based on any combination of three organizational dimensions:
   1. Geographic jurisdiction – defined with areas/geofences
   2. Domain jurisdiction – defined with Incident types
   3. User jurisdiction – defined with groups
5. The system shall allow to define agency’s/control center’s jurisdiction over any geographical area (polygon/geofence). This geographical jurisdiction will define responsibility to incidents that are created in the area. Any area can be assigned to any number of control centers (many to many).
6. The system shall allow to define agency’s/control center’s jurisdiction over any Incident type. This will define responsibility of agency to incident types based on the domain of expertise. Any incident type can be assigned to any number of control centers (many to many).
7. The system shall allow to assign groups (of users) to jurisdiction of control center/agency. this will define the permission and responsibility of control center to view, dispatch, message and manage groups of users. Any group can be assigned to any number of control centers (many to many).
8. The system shall display for each center/agency the amount of dispatchers, responders, Reporters and SOS users currently under its jurisdiction.
9. The system shall allow to define for each control center a call-in phone number and geographical geofence for incoming SOS calls. When users activate an SOS signal, the mobile app will dial a number based on the location of the user.
10. The system shall allow to define for each control center its default map focal point and zoom level.
11. The system shall allow to copy control center attributes from another control center (in order to simplify the creation and management of control centers).
12. The system shall allow the administrator to archive control centers and define who will have access to archived control centers.

## Branding – Icons & Logos

1. The system shall allow uploading customized icons and associate them with multiple UI entities in the system (i.e. users, roles, group, equipment, incident types etc.).
2. The system shall allow uploading customized logos to be displayed in the dispatcher screen and on the mobile app.

## SMS/Email Configuration

1. The system shall allow administrators to define API parameters for SMS and email via the user interface (select for which situation to send an SMS message to assets, contacts and users). SMS messages packages to be purchased separately if requested.
2. The system shall support multiple SMS gateway providers, allowing a simple process of identification to the SMS gateway API service.
3. The system shall allow to define multiple message templates.
4. The system shall allow to define sending an SMS to assets and contacts on multiple triggers/scenarios:
   1. On every dispatch failure (i.e no data network available). This SMS will include details of the incident as well as a link to the application.
   2. On every dispatch (i.e. backup for app dispatch).
   3. To users dispatched to an incident that do not have the system’s dedicated app.
   4. On every message or message failover.
   5. On status updates of responders in an incident (i.e. notify all other relevant contacts of change in status).

# Maps/GIS Settings

## GIS Map Configuration

1. The system shall support Google Maps GIS infrastructure.
2. The system shall allow the configuration of the map’s default layers including layers of incidents, users, POIs, units, assets, areas/geofence/polygons, traffic conditions, Google street view).
3. The system shall allow to measure distances between two way-points both aerial distance and routing-based distance with driving directions).
4. The system shall allow to click on the map (pin) and retrieve the address (reverse geocode).
5. The system shall allow the configuration of the map’s default type (street, satellite, hybrid).
6. The system shall allow the limitation of address search results to display only address within a specific jurisdiction (appending a text to the geocode query such as name of city, state, country etc.).
7. The system shall allow to define for each control center its default map center and zoom level.
8. The system shall allow the configuration of an external ESRI ArcGIS server map/mxd - allowing the overlay of that map in the dispatcher web application.

## GIS POI Configuration

1. The system shall allow the administrator to create points of interest (POIs), allowing dispatchers to present them on the map and/or associate new incidents to them.
2. The system shall allow the definition of a name, icon, address, tag, description and coordinates for each POI.
3. The system shall allow the administrator to associate one or more asset/contact to each POI allowing dispatchers to see the details of assets/contacts associated with the POI. Assets may include sensors and devices located in the POI. The system shall allow to access external links or data that are associated with the assets (camera footage etc.).

## GIS Polygon/Geofence Configuration

1. The system shall allow the administrator to draw geofences/ polygons on the map. The system shall allow dispatch operators to present geofences on the map and to associate multiple system entities to the geofence: incidents, users, POIs, units, assets, alert levels.
2. The system shall allow the definition of a name, color and tags for each polygon/geofence.
3. The system shall allow the administrator to create one or more asset/contact for each polygon allowing dispatchers to see the details of contact/assets associated with the polygon.
4. The system shall allow the administrator to create a polygon using a drawing tool (freehand).
5. The system shall allow the administrator to create a polygon by defining a POI and a radius around the POI (circle).
6. The system shall allow the configuration of alerts per area/geofence if the number of users with specific roles or equipment does not match a required amount (‘staffing alert’).
7. The system shall allow the configuration of alerts per area/geofence if for a period of time any specific role or equipment has been missing in the area (‘absence alert’).
8. The system shall allow to activate an alert or a distress signal or an incident when a user enters or exits a geofence.
9. The system shall allow the administrator to define three graduated levels of readiness (alert levels) for each geofence. The system shall allow to display the alert level for each polygon on the map as the polygon color (red=high, yellow=medium, green=low).
10. The system shall allow the administrator to define for each geofence a designated phone number that will be automatically dialed by a user in distress who is located in that geofence.

# Incident Management Settings

## Incident Configuration

1. The system shall allow the administrator to configure one or more incident type using the user interface.
2. The system shall allow associating each incident type with a unique ID, name, tags, icon and additional specific properties.
3. The system shall allow to define for each incident type a priority level 1-5 (1 being the highest level).
4. The system shall allow each incident type to be associated with one or more form templates.
5. The system shall allow to define for each incident type an SLA (service level agreement) that includes three time parameters:
   1. The first SLA defines the expected time for an acknowledged dispatch of a responder to an incident
   2. The second SLA defines the expected time for arrival of first responder at the incident
   3. The third SLA defines the expected time for completion of the incident by the responder
6. The system shall trigger a visual and audible alert on any deviation from SLAs.
7. The system shall allow to associate contacts/assets to the incident type (i.e. an expert for this type of incident).
8. The system shall allow the soft-delete of incident types.
9. The system shall allow filtering the list of incident types.

## Auto Dispatch Rule Configuration

1. The system shall allow administrators to set up an automatic dispatch rule for each incident type. This dispatch rule can be comprised of one or more sub-rules.
2. The system shall allow the configuration of a sub-rule that will dispatch one/more/all users that have a specific role, group or equipment.
3. The system shall allow each sub-rule to be limited to users within a specific ETA.
4. The system shall allow each sub-rule to be limited to users that are associated to the incident geofence/polygon (in their user profile).
5. The system shall allow each incident rule to be limited to a time counter (after the time elapsed the automatic dispatch engine will not dispatch additional users to the incident).
6. The system shall allow to define for each incident rule a skip time - the time when additional resources will be dispatched in the incident if the previously dispatched user does not respond.
7. The system shall allow each incident rule to include a defined waiting time (the amount of time the incident will be displayed on responders’ mobile devices before incident is no longer available to responder).
8. The system shall allow the automatic dispatch of additional resources if the initial dispatched users will reject the incident.
9. The system shall allow to define for each incident type the following criteria for dispatch:
   1. Whether the incident is a singular (one by one) or multitask (meaning the responder can be dispatched to more than one incident at any given time)
   2. Whether to prioritize responders with lower load of pre-existing incidents
   3. Whether to calculate responder’s ETA based on the location of the responder at the end of the last incident
   4. Whether to avoid dispatching the responder to other incidents
10. The system shall allow to define for each incident type a list of statuses that the dispatcher or responder can send during the incident. For each status the Administrator can define how the report will appear in the dispatch center - as a popup, with or without an audible alert.
11. The system shall allow the definition of pre-condition for each and between dynamic statuses (e.g. the user will be allowed to report ‘need additional resources’ only if the ‘on-scene’ status was previously reported).

## Dynamic Forms for Incidents

1. The system shall allow the definition of dynamic form templates for each incident type.
2. The system shall allow the definition of a dynamic forms in multiple languages.
3. The system shall allow administrators to create a form using a drag and drop user interface.
4. The system shall support the following field types in dynamic forms:
   1. label/header
   2. simple text box
   3. text area box
   4. checkbox
   5. radio buttons
   6. location coordinates
   7. date & time
   8. current timestamp
   9. take photo with camera
   10. upload photo from desktop
   11. video
   12. electronic signature
   13. drop down (pick from list)
   14. auto complete from list
   15. scan barcode/QR code
   16. separators
   17. Index
5. The system shall allow to define specific fields as mandatory. Failing to fill a mandatory field will display an alert and prevent dispatch operator from closing an incident.
6. The system shall allow preconditioning for fields, meaning that specific fields will only appear if another field meets the precondition.
7. The system shall allow the definition of field level limitation for text boxes allowing the users to enter only numbers, chars etc.
8. The system shall allow the definition of auto-complete of text boxes from internal or external data sources (via database or web services).
9. The system shall allow the definition on a field level of read-only attributes.
10. The system shall allow the definition on a field level of API header (defining the field name/XML tag for system-to-system integration).
11. The system shall allow the definition on a field level if each field will be available for Dispatch Operator, Responder, Reporter users, allowing to enter data into this field.
12. The system shall allow the definition on a field level of the length of text fields.
13. The system shall allow the editing, duplicating and modifying of existing forms.
14. The system shall allow the soft delete of existing forms.
15. The system shall allow the user to enlarge the form text size.
16. The system shall allow to define an index sidebar for quick navigation in form.
17. The system shall allow night mode for forms (bright text on dark background).
18. The system shall allow the association of a dynamic form to multiple incidents.
19. The system shall allow the form editor to open a preview of the form as it would appear to the users.

## Incident Dynamic Situation Reports Configuration

1. The system shall allow the creation of dynamic situation reports including report name, icon, and specific parameters.
2. The system shall allow mobile users to send situation updates from the app main dashboard (e.g. check-in, check-out, stuck in traffic etc.).
3. The system shall support two formats for situation updates:
   1. Header only
   2. Header with open text
4. The system shall allow to trigger for specific situation updates a visual and audible alert on the dispatch operator screen.

# Dispatcher/Operator Desktop Application

## General UI Guidelines

1. The desktop app should be fully web-browser-based running on Google Chrome with no local installations.
2. The system shall support multiple arrangements of the layout of panels/elements on the screen:
   1. Allowing to turn on/off which panels are displayed to the user.
   2. Allowing the user to arrange where each panel will be placed in the user’s screen.
   3. Allowing to display each panel in multiple sizes – full screen, half screen, quarter screen and floating.
3. The system shall allow a search/auto-complete on map and all other panels of multiple entities in the system (addresses, points of interest, users, groups, roles, equipment, units, incidents, assets, geofences).
4. The system shall allow to limit searches of addresses to a specific area.

## Login & Access Control Security

1. The systems shall allow to assign each dispatcher/operator specific control centers. When logging-in the operator is displayed only the assigned control centers to log into.
2. The system shall allow to assign each operator/dispatcher a permission profile which will define access to the various menus and capabilities in the system (for example a user without administrator permissions will not be able to view the setup screens).
3. The system shall allow to enforce a strong password for login.
4. The system shall allow to enforce Captcha screen upon logging in.
5. The system shall allow the user to reset the password via “forgot password” email which will be sent to a predefined user’s email.
6. The system shall allow a user to change the password after login.
7. The system shall allow limiting login to specific IP addresses of the computer logging-in from.

## Users Panel/Grid

1. The system shall allow the operator to define and edit user details such as:
   1. Name and alias/code
   2. Photo and user icon on map
   3. Associated groups, roles & equipment
   4. Number of active incidents the user is enrolled in
   5. Recent user availability state
   6. Latest location updates
   7. Communication and mobile app status
   8. Licenses and Permission profile
   9. Addresses and associated geofences
   10. Relationships with other entities in the system
   11. Policies
   12. Emergency contacts
   13. Recent activity and performance statistics
2. The system shall allow to send smart messages to user.
3. The system shall allow the operator to post to user’s log user updates.
4. The system shall allow to filter/sort the users panel according to multiple properties:
   1. Personal details: name, phone, username
   2. Location details: address, geofence
   3. Organizational details: Profile, Group, Policy, Role, Equipment, Control Center
   4. Mobile device parameters: App license, Version, Device, Availability, Locations received within past time
   5. User Updates: user update type and timeframe user update was sent or not sent
5. The operator can select multiple users on the users panel and perform actions such as:
   1. Sending a smart message
   2. Changing Policies
   3. Export to Excel

## Operations (Incidents) Panel/Grid

1. The system shall allow users to view a list of active incidents and their status based on permissions.
2. The system shall allow user to sort/filter the incident grid based on various parameter such as type, date, dispatcher, active responders, source, location & status.
3. The system shall allow the user to close or cancel incidents from the incidents grid.

## Operational Map & Geofencing Management

1. The system shall allow to view multiple layers (users, units, incidents, POIs, geofences) on the map.
2. The system shall allow selecting the color and opacity of each geofence on the map.
3. The system shall allow to switch the map to a geofence marking mode - using a tricolor code to mark each zone (i.e. clear, danger, etc.).
4. The system shall allow the user to select a satellite map view, street map view or a hybrid view.
5. the system shall allow the user to search on the map for addresses, users, incidents & POI.
6. The system shall allow filtering elements on the map based on tags.
7. The system shall allow user to open “Google Street View” (where available).
8. The system shall allow a user to open an incident on the map via drop pin.
9. The system shall allow the user to measure the distance between points on the map.
10. The system shall allow the user to get directions between points on the map.
11. The system shall allow the user to view information about each geofence (polygon) defined in the system including the number of active incidents, available users, units, assets.

## Resources Monitor

1. The system shall allow the dispatch operator to display a panel that presents areas (geofences) with real-time details of the system resources currently located in each area: users, assets, incidents, units.
2. The system shall allow the dispatch operator to draw a geofence on the map and immediately present all resources currently in the geofence: users, assets, incidents units.
3. The resources monitor shall display the aggregated number of the user, assets, units and incidents and a gauge that reflects the current status of the resources.
4. The resources monitor shall allow the operator to drill down and view the details of the resources.
5. The resources monitor shall allow to send a message to the users that are located in a geofence.

## Alerts & Notifications

1. The system shall have a dedicated alert / notification panel.
2. The system shall allow to define different sounds for different alert categories.
3. The system shall allow to define the behavior for each alert type - alert counter, play sound on desktop, alert popup.

The system shall support the following notification types:

* 1. Incident related alerts:
     1. Incidents created by 3rd party/reporter
     2. Modifications to incident type or incident location
     3. User reporting “on scene” while actually not being in the correct address.
     4. Incident SLA not met (late on dispatch, on arrival or on completion)
     5. New form filled.
     6. Mismatches or other issues in forms
     7. SOS/distress signal
  2. Geofencing related alerts:
     1. User entering/exiting a geofence border
     2. Geofence with not sufficient staffing/resources (users with specified roles)
     3. Geofence absent of a specific resource (users with specified roles)
     4. Geofence exceeding maximum capacity
     5. New video streaming in
  3. User related alerts
     1. User Updates from users
     2. User not moving for predefined time
     3. Lack of communication with user for specified time
     4. User mobile device with low battery level

## Incident Creation/Call Taking

1. The system shall allow the creation of an Incident via the following methods:
   1. “Create Incident” panel
   2. Dropping a pin on the map and selecting “Create Incident”
   3. Through mobile Reporter app
   4. Through APIs and third party devices/systems interfacing with the Dispatcher
   5. Through triggers set in the system (create incident in case of violation of rules)
2. The system shall allow to access an existing Incident via the following methods:
   1. Searching for an incident in the Search module
   2. Clicking on an incident row in the Incidents Panel
   3. Clicking on the incident preview popup in the Map panel
   4. Via a third party system API that triggers the Incident Management Panel of a specific incident.
3. The system shall support displaying incidents in Draft status that are missing either location or Incident Type.
4. The system shall support multiple time-zone Incident.
5. The system shall allow to enter details of caller (one or multiple), including phone number, name and comments.
6. The system shall support ability to collect caller’s details via phone/PBX system (requires dedicated interface with PBX).
7. The system shall alert if there are suspected duplicate callers based on name or phone number within a given timeframe.
8. The system shall allow for entering the incident location via various methods:
   1. Incident location from text - auto-complete search based on GIS data. The location search can auto-complete from a combination of addresses and/or points of interest and/or roads. Once the location is chosen, the system shall display a map centered on the location.
   2. Incident location from map: The system shall allow an incident’s location to be entered by “pinning” the map.
   3. Location details and comments - customizable fields such as entrance, floor, name etc.
   4. Where available, the system shall allow the display of other location imagery such as street view, POI details and blueprints etc.
   5. The system shall display location coordinates in various coordinate methods.
   6. The system shall support incidents with 2 addresses/waypoints (origin-destination).
   7. The system shall support incidents with dynamic (moving) location (incident following location of a caller or user that activated SOS alert).
9. The system shall indicate if the caller or location details match similar data of incidents in the past. In such instances, the system shall allow users to view the historical incident.
10. The system shall indicate if caller or location details match similar data of another current open incident. In such a case, the system shall display an alert for suspected duplicate incidents and allow the operator to merge the two (or more) incidents.
11. The system shall allow for entering incident details via the following methods:
    1. Incident type/code – combination field of auto-complete and dropdown list from a predefined list of incident types grouped by tags.
    2. Incident comments – free text field.
    3. Incident details/forms - from predefined forms associated with the incident type.
12. When selecting the incident type, the system shall automatically display the following:
    1. A dynamic checklist/form/s with fields guiding the dispatcher as to the recommended steps.
    2. Incident priority. Dispatcher can override the predefined priority (if granted permission).
    3. Incident predefined SLAs - expected dispatch, arrival and completion time. The system will indicate whether the SLA is expected to be met by the dispatched users (based on whether ETA meets SLA).
    4. Available dynamic statuses (available statuses are updated continuously based on the incident state).
    5. Available predefined form/s allowing the dispatcher to populate the form fields with relevant data.

## Dispatching

1. For each Incident type, the system shall allow a Response Protocol to be defined with the optimal response for each Incident Type. The protocol may include any combination of the following:
   1. Who - Various types of resources, roles, equipment, groups
   2. How many – All available or a specific number or all available resources
   3. Limitations - limiting dispatch to a required ETA (time of arrival) or to resources that are associated with the area/geofence in which the incident was created.
   4. When – immediately or with a delay timer
2. Once a location and Incident type are entered, the system shall automatically search and display recommended available resources that match (or almost match) the Response Protocol criteria.
3. The recommended resource list will be displayed sorted by their distance from the incident location. The resources (users and units) shall be displayed with all their parameters (roles, equipment and current status). The specific parameters that match the incident requirements shall be highlighted to emphasize their relevance to the incident.
4. The system shall allow the Dispatcher to modify ad-hoc the pre-defined response protocol. Modifying the protocol will automatically update the recommended dispatch list.
5. At any stage, the system shall allow the Dispatcher to activate the automatic dispatch protocol and/or manually dispatch specific resources.

## Incident Management & Progress Gauge

1. The system shall display a clear view of the incident status including:
   1. Progress - current stage of incident: call taking, data entry, dispatch, on scene management, forms and logs of event.
   2. User statuses - each user that is dispatched to the incident can update current status. The statuses are available on display to all other participants in the Incident.
   3. Not optimal response - the system shall alert the Dispatcher to a lack of adequate response based on the predefined response protocol.
2. The system shall allow to enter incident notes/logs. These free-text logs are saved in the system with a timestamp and can also be sent as flash updates to other users active in the incident.
3. The system shall allow dispatcher to send predefined situation updates (reports) to incident log and other users active in the incident.
4. The system shall allow dispatcher to send and receive from active users real-time audio recordings via the PTT Channels feature.

## Other Dispatch Tools

1. The system shall allow users to search and display location history (breadcrumbs) of active users in the incident with a click of one button. The users’ locations can be animated to display the movements of the users on the map.
2. The system shall allow the Dispatcher to view and modify any Incident information (location, caller details, incident type, forms).
3. The system shall allow the Dispatcher to manually update the mobile user’s status in incident.
4. The system shall allow the Dispatcher to cancel a dispatch and send abort message to mobile user.
5. The system shall allow the Dispatcher to share an incident with other Dispatchers in other Control Centers in cases where the predefined jurisdiction rules exclude the other Dispatcher from viewing the incident. The share tool will send a notification and alert to relevant dispatchers.

## Assets - Incident Intelligence

1. The system shall constantly search for information and data regarding assets that can be relevant to the Incident management. For instance, when the location is entered, the system shall search in history for other incidents with same (or close) location. The system shall also identify assets that can be relevant to the incident based on various types of relationships: location. expertise, a person involved in the incident (caller, reporter) etc.
2. The system shall search for sensors, cameras and other detection devices that are located in the incident’s area (defined as assets linked to Geofences or POIs near incident location). The details of these sensors and camera (and access link where relevant) shall be made available to the dispatcher in order to enhance the situational awareness and decision making.
3. The system shall allow to create a new asset “on the fly” and link the new asset (or an existing asset) to an incident.
4. The system shall have an Asset management panel to create and edit all assets in the system. The asset’s parameters shall include: Name, alias, category, type, status, location, relationships with other entities in the system, ways to communicate and activate the asset, historical activity of the asset and its involvement in any incidents in the past.

## Forms - Incident Data Collection

The system shall allow to the association of Dynamic Forms (one or multiple templates) to any Incident Type. Once the incident type is chosen, the relevant form template will be displayed. Form fields can be shared amongst all active participants in the Incident (Dispatcher, Mobile Users, 3rd party through API). The Dispatcher and Mobile User will be required to fill in mandatory fields. Updated fields will be immediately displayed to all active participants.

## Incident Log and Data Summary

1. The system shall allow the Dispatcher and any other authorized manager to view the detailed incident log.
2. The log shall include each and every action performed during the incident with a timestamp.
3. The system shall provide a detailed timetable grid displaying the following timestamps for all active responders in the incident:
   1. Original ETA (ETA on time of dispatch)
   2. Time dispatched
   3. Time en-route
   4. Time on scene
   5. Time done
4. The timetable grid shall allow Dispatcher to complete any missing timestamps.
5. The system shall allow Dispatcher and Responder (from within the app) to produce and export a PDF file summarizing the details of the incident.

## Scenario/Event Planning

1. The system shall allow the administrator to plan large-scale planned events. Each Scenario includes multiple phases and tasks.
2. Scenarios can be pre-scheduled to a specific date, set to a recurring pattern for series of activations.
3. The system shall allow to define one or more phase for each scenario.
4. The system shall allow to define one or more task for each phase.
5. The system shall allow to set the timing for each task in relation to the scenario activation time.
6. The system shall display the scenario plan as a table and as a Gantt chart
7. The system shall allow to define locations for scenario tasks by addresses, point on the map or predefined POIs.
8. The system shall allow to define a designated priority (1-5) for each scenario task.
9. The system shall allow each scenario task to be defined as either automatic or manual dispatch.
10. The automatic dispatch engine will be able to assign and dispatch users to the scenario incidents based on the above defined priority.
11. When launching a new scenario, the system shall prompt additional credentials (password entry).
12. The system shall present a summary of all potentially dispatched resources when planning the scenario (calculate the amount of dispatched responders based on the pre-defined automatic dispatch rules).

## Smart Messaging

1. The system shall allow the Dispatcher and Supervisor to send Smart Messages to individual Mobile users or to a group of mobile users.
2. The system shall display the status of each message, including whether the message was received by the mobile device, when it was read, whether the user replied and the content of the reply.
3. The system shall allow all message statuses to be automatically refreshed and exported to a spreadsheet.
4. The system shall allow message Sender to define if message is high priority.
5. The system shall allow the message Sender to define an expiration date for the message.
6. The system shall allow several different types of Smart Messages, including:
   1. Simple text message - asking mobile users to confirm receiving the message.
   2. An open question - asking mobile users to fill in their answer.
   3. A multiple answer question (survey) - asking mobile user to pick from a list of answers.
7. Location check - The sender can add to each message a request that recipients share their location.
8. The system shall allow to create predefined templates for messaging. These templates shall be accessible from both the Dispatcher platform and Supervisor mobile app.
9. The system shall allow to attach pictures and files (PDF, DOC, XLS etc.) to a message. The files could be opened by the mobile.

# Mobile Application

## Mobile Application Modularity and Basic Functionality

1. The system shall allow for the assignment of different mobile modules for each mobile user. Each module will provide the users with a different set of features and interaction options with the system. The configurations include:
   1. A Supervisor module, allowing to view on a dynamic map all available users, incidents, assets, units and POIs, to send and view replies of smart messages to authorized groups of users and to activate deactivate triggers during an incident.
   2. A Responder module, which shall allow the users to be dispatched to an incident, to report multiple statuses, fill dynamic forms, chat (voice and text) with other co-responders and view information relevant to the incident (status of other responders, location of nearby POIs and assets etc.).
   3. A Reporter module, which shall allow the users to report an incident to the dispatcher. The incident types that can be reported are configured in the dispatcher in the incident setup section. Permissions allocated to each mobile user will determine the whether the following functionality is available to the user:
      1. The ability to report an incident from a location other than the user’s current location.
      2. The ability for the users to dispatch themselves to the incident they are reporting.
      3. The ability for the users to activate the auto dispatch rules for the incident type that they are reporting.
   4. An SOS module, which shall allow the users to log into a dedicated app for SOS activation in the case of emergencies. Permissions allocated to each mobile user will determine if this app is an active or passive SOS app:
      1. Active SOS will allow the user’s locations to be tracked at all times that the user is logged into the application.
      2. Passive SOS will allow the user’s locations to be tracked only during the time period when a user activates an SOS incident until the time where the user is no longer in danger (i.e. the incident has been closed by the Dispatcher).
   5. A PTT Channels module allowing users to communicate with colleagues with voice and text.
   6. A Messaging module, which shall allow the users to receive messages from the dispatcher and to either acknowledge the message or respond to the message, based on the message type.
   7. An Asset Lookup module shall allow the app user to search for nearby or remote assets and perform tasks and actions on these assets.
   8. An ‘Escort Me’ module shall allow the app user to activate an escort countdown and be monitored by dispatch.
   9. A Map module shall allow the app user (with appropriate permission) to view nearby resources.
2. The system shall allow users to login with their assigned username and password.
3. The system shall allow enforcing a strong password for app login.
4. The system shall allow mobile users to send logs to support for troubleshooting.
5. The system shall allow the users to view system information.
6. The system shall allow the users to sync their app with the server.
7. The system’s mobile user interface will be defined based on the device’s local language settings (for supported languages).
8. The system’s user interface shall be similar across multiple platforms (e.g. iPhone, Android) to simplify user training and adaptation.
9. The app should be able to rum on iPad with customized landscape (horizontal) orientation.
10. The user shall be able to download the mobile application via the commercial App Stores (e.g. Apple App Store, Google Play).
11. The user shall be able to use existing devices without requiring any special modifications (assuming operating system is supported and, data plan, push notification and location services are enabled).
12. The system shall allow the Admin to upload the organization’s logo to be presented on the desktop and mobile.
13. The system shall allow the administrator to determine if the user is allowed to log out of the application.
14. The system shall allow the administrator to determine if users are allowed to change their status to offline.
15. The system shall prevent users from logging into more than one mobile device at a time with the same user name and password. Logging in to a second device will automatically force logout on the former device.
16. The system shall allow to register the mobile device’s MAC address to the server.

## Mobile Status, Locations and Communication Check

1. The mobile app shall allow the user to report various availability statuses for receiving assignments.
2. The system shall allow the Admin to define the most suitable location update accuracy and intervals in order to balance battery consumption with location updates.
3. The system shall allow the Admin to define 3 thresholds for the age of user’s locations in order to distinguish most updated locations from older less updated locations.
4. The system shall allow the Admin to define what age of location would be considered unreliable for Dispatch.
5. The system shall allow users with appropriate permission to switch their active location update to a fixed location for a specified period of time after which the locations update will reinitiate.
6. The system shall monitor the time lapse from app’s communication with the system’s server.
7. The mobile app shall allow Admin to define what age of communication would be considered unacceptable thus displaying an alert for apps that haven’t communicated with the server for X amount of minutes.
8. The system shall allow the app user to update its mobility platform (vehicle, bike, pedestrian etc.)
9. The system shall allow the app user to join a unit.

## Mobile SOS

1. The system shall allow the user to activate an SOS alert incident.
2. The system shall provide the user with a 5 second buffer so user can cancel the SOS alert if it was activated accidentally.
3. The system shall automatically dial a phone number configured by the command center when the SOS is activated. The dialed number can be set to change depending on the mobile device’s location.
4. The system shall continue to attempt to send the incident details to the dispatcher (retries) even if the user is in an area where there are connectivity issues.
5. The system shall allow the user to initiate another call to the phone number configured by the command center if the caller is unable to get through initially or if the caller needs to call again.
6. The system shall change the application background colour to red during the time that the SOS incident is active.
7. The app shall automatically activate video streaming from the app to dispatch center when entering SOS mode.
8. The app shall allow the user to chat with dispatch and responders en-route.
9. The app shall allow the user to communicate via audio PTT with dispatch and responders.
10. The system shall allow the user to cancel the SOS call after it has been activated by typing the user password into the application.
11. The system shall allow the user to choose the option to activate an SOS incident automatically upon launching the application.
12. The system shall track the users’ locations depending on their assigned permissions.
    1. Passive SOS users will only be tracked when they are active in SOS incidents. At this time, the locations will be tracked with high accuracy
    2. Active SOS users will be tracked at all times based on significant change, unless they activate an SOS incident, whereby their locations will be tracked with high accuracy.
    3. The system shall send a message to the user from the dispatcher if the SOS incident is closed by the dispatcher before the user has deactivated the SOS from the mobile application.

## Mobile Reporter

1. The system shall allow the users to send an incident report to the dispatcher from their current location.
2. The system shall allow the users to create an incident from a different location if they have the permissions to do so.
3. The system shall allow the administrator to limit the search results for addresses in the reporter to a particular area.
4. The system shall allow the users to fill in and send dynamic forms when creating the new incident (if the incident type selected has an attached form).
5. The system shall allow the users to dispatch themselves to the new incident if they have the permissions to do so.
6. The system shall allow the users to activate the auto dispatch protocols for the new incident if they have the permissions to do so.
7. The system shall allow the users to dial the phone number configured by the command center after they have opened the new incident.
8. The system shall allow the users to dial the phone number configured by the command center if the new incident is unable to be created due to connectivity issues.
9. The system shall provide the users with all the functionality of the SOS module.
10. The system shall track the users based on their permissions profiles
    1. Users with the reporter module and the passive SOS module shall only be tracked when they are active in SOS incidents. At this time, the locations shall be tracked with high accuracy.
    2. Users with the reporter module and the active SOS users shall be tracked at all times based on significant change, unless they activate an SOS incident, whereby their locations shall be tracked with high accuracy.
    3. Location sampling rate and accuracy can be defined remotely by Administrator. Different levels of rate and accuracy can be defined for each status of user: routine, active in incident, Reporter, SOS mode etc.
11. The system shall allow the users to activate an SOS incident in case of emergency.
12. The system shall allow users with the reporter module to also have access to the Supervisor, Responder and Messages if they have the permissions to do so.

## Mobile Responder

1. The system shall allow the users to view the responder dashboard.
2. The system shall allow users to change their availability status based on their current availability.
3. The system shall allow users to change their mobility type based on their current method of transport.
4. The system shall allow the users to send dynamic status updates to the dispatcher.
5. The system shall allow the users to view all the details of their user profile.
6. The system shall allow the users to receive push notification, splash notices with all incident details (type, time elapsed, location, comments, additional users’ statuses-qty).
7. The system shall allow the users to receive push notifications for new incidents even when the application is closed.
8. The system shall activate a siren when users are dispatched to incidents which will ring until the user acknowledges receipt of the incident.
9. The system shall allow the users to receive notifications via sync, if they are not received via push notifications.
10. The system shall allow the users to respond to incidents they have been dispatched to (acknowledge, en-route, on-scene, done, abort and pre-conditioned dynamic statuses).
11. The system shall allow the users to navigate to the incident location using navigation apps available on the users mobile devices (i.e. Waze, Google maps, Apple maps).
12. The system shall allow the users to activate phone video camera and stream live video to dispatch from scene.
13. The system shall allow the users to view a list of all incidents that they have been dispatched to (active, postponed, closed).
14. The system shall allow the users to view and fill in dynamic forms (if the incident type has an attached form).
15. The system shall allow the users to update the incident location to their current location if they determine that the location is different to the one shows in the incident details.
16. The system shall allow the users to receive notifications of changes in incident location.
17. The system shall allow the users to receive flash updates sent by the dispatcher.
18. The system shall allow the users to receive notifications if the dynamic form was updated by the dispatcher or another user.
19. The system shall allow the users to receive notifications of change in incident type.
20. The system shall allow the users to view the details of the incident source (name and phone number).
21. The system shall allow the users’ locations to be tracked. Users shall be tracked at all times based on significant change, unless they are active in an incident (en-route, on-scene) or activate an SOS incident, whereby their locations will be tracked with high accuracy.
22. Location sampling rate and accuracy can be defined remotely by Administrator. Different levels of rate and accuracy can be defined for each status of user: routine, active in incident, in SOS mode etc.
23. The system shall allow the users to view system information and location details.
24. The system shall allow the users to activate an SOS incident in case of emergency.
25. The system shall allow users with the Responder module to also have access to the Supervisor, Reporter and Messages if they have the permissions to do so.

## Mobile Supervisor

1. The system shall allow the Administrator to grant Supervisor permission to users. Each Supervisor can be assigned specific authority of a jurisdiction over groups of users, over designated geographic areas or incident types.
2. The system shall allow the Supervisor to view a map showing all authorized incidents depending on the level of authorization of the Supervisor.
3. The system shall allow the Supervisor to view a map showing all authorized users who are logged into the app and are either available for dispatch or are active in incidents. The users displayed to the Supervisor will depend on the level of authorization of the Supervisor.
4. The system shall allow the Supervisor to lock the map focus to center on another user.
5. The system shall allow the Supervisor to view a map showing all Points of Interest created by the organization.
6. The system shall allow the Supervisor to view a map showing their location on the map.
7. The system shall allow the Supervisor to tap on the incident or user icons on the map and see a pop up containing additional information such as address and phone number of the user.
8. The system shall allow the Supervisor to view a grid of all incidents open in the dispatch center along with the most relevant status of the users in the incident.
9. The system shall allow the Supervisor to filter the incidents seen in the grid based on time since the incidents were opened.
10. The system shall allow the Supervisor to filter the incidents seen in the grid based on the proximity of the incidents to the users’ location.
11. The system shall allow the Supervisor to activate an SOS incident in case of emergency.
12. The system shall allow users with the reporter module to also have access to the Responder, Reporter and Messages if they have the permissions to do so.
13. The system shall allow the Supervisor to send a smart message from the mobile app to groups and users in the system.
14. The system shall allow the Supervisor to release predefined triggers in an incident from the mobile app. Releasing a trigger can activate a predefined dispatch sequence.
15. The system shall allow the Supervisor to cancel active incidents from the mobile app, thus aborting any active Responders in the incident.

## Mobile Messaging

1. The system shall allow all users to have the option to receive messages from the dispatcher.
2. The system shall allow all users to read and respond to messages sent by the dispatcher.
3. The system shall allow users to view all messages sent by the dispatcher.
4. The system shall allow users to confirm receipt standard messages by clicking the “OK” button.
5. The system shall allow users to answers open-ended message by typing a reply.
6. The system shall allow users to answer a questionnaire/survey message by selecting one or more pre-defined answers.
7. The system shall allow users to send their current location as a reply to a location request message.
8. The system shall allow users to confirm their communications are working as a reply to a communication check message.

## Mobile Asset Lookup

1. The app shall allow users with permission to search for nearby Assets.
2. The app shall allow users with permission to search for assets belonging to specific asset types (i.e. cameras, hydrants etc.).
3. The app shall allow users to search for asset IDs (i.e. vehicle number plates, personal IDs) and match them with databases. If there is a match - the app shall allow the app user to add a log entry for that asset or create an incident associated with the asset. If there is no match - the app will allow the user (with permission) to create a new asset and save it to the asset DB with all its attributes (name, address, photograph etc.)

## PTT

1. System shall allow Responders and Dispatchers to communicate with voice and text messages via a Voice Over Push To Talk (VoPTT) module. The system shall allow users to view dashboards and reports.
2. PTT Chat Rooms (PCR):
   1. The VoPTT module shall allow Administrators to create a “PTT Chat Room” (PCR) for any of the predefined groups.
   2. The VoPTT module shall create ad-hoc PCR for evolving incidents in order to facilitate voice communication amongst the members of the incident.
   3. The VoPTT module shall allow authorized Responders to create personal PCRs with colleagues and members.
3. PTT Chat Room details - The VoPTT module shall display for each PCR the following details:
   1. PCR title
   2. PCR member's count
   3. PCR members list
   4. PCR current status - active or silent
4. PTT Chat Room members:
   1. The VoPTT module shall allow authorized users to create/close new chat rooms.
   2. The VoPTT module shall add automatically new members to ad-hoc incident based chat rooms as they confirm dispatch to an incident/event/unit.
   3. The VoPTT module shall allow authorized users to add/remove members from groups
   4. The VoPTT module shall allow any user to view the names of other members in shared PCRs.
5. PTT voice management:
   1. The VoPTT module shall allow to silence/reactivate any PCR
   2. The VoPTT module shall allow user to view when a PCR is active
   3. The VoPTT module shall allow any authorized user to push to talk (other users will only be able to listen).
   4. The VoPTT module shall allow authorized users to replay recordings.
6. Performance:
   1. The VoPTT module shall support at least 50 active PCRs simultaneously
   2. The VoPTT module shall support concurrency of 20,000 users
   3. If user loses connectivity, the VoPTT module will allow to download missed recordings and play them.

## Escort Me

1. The mobile app shall include an Escort function which shall allow the mobile user to activate an escort timer that will indicate to dispatch he wishes to be monitored.
2. The timer will switch the user’s status to ‘escort me’ and the user’s location will be sent to the server.
3. The timer will run both on the mobile app and on the server independently.
4. As the countdown timer approaches the end (zero) an alert will indicate to user to either cancel escort mode or extend the timer.
5. If that countdown timer reaches zero without the user turning off the feature, an SOS alert will be triggered in the dispatch center.
6. The SOS alert will be triggered even if the device was turned off or destroyed during the countdown.
7. The system can be configured to indicate which users are in “Escort” mode and present them on the map.