



SERVICE DEFINITION

Review Date: 01/01/2027

Table of Contents

Company and Contact Information	2
1. Overview	2
2. Service Features	3
2.1 Core Functionality	3
2.2 Integrations (subject to availability)	3
3. Data Backup, Restore, and Disaster Recovery	3
3.1 Data Backup	3
3.2 Data Restore	4
3.3 Disaster Recovery	4
4. Onboarding & Offboarding	4
4.1 Onboarding	4
4.2 Offboarding	4
5. Service Constraints	5
5.1 Maintenance Windows	5
5.2 Maintenance Management	5
5.3 Customisation	5
5.4 Connectivity	5
5.5 Integration	5
6. Service Levels	6
6.1 Availability	6
6.2 Performance	6
6.3 Support hours	6
7. After Sales Support	6
8. Technical Requirements	7
8.1 Minimum system requirements (Operations Dashboard)	7
8.2 Minimum system requirements (Staff Mobile App)	7
9. Hosting Options	7
10. Security	7
11. Termination of Contract	8

Company and Contact Information

Crown Integrated Services is a Limited Company registered at UK Companies House registered Number: 14446453.

Crown Integrated Services Ltd are registered for VAT. The VAT registration number is 427 2448 94, registered at: West House, King Cross Road, Halifax HX1 1EB

Email: admin@crownis.com

Tel: +44 (0)7802 305466

Crown Integrated Services Ltd holds insurance for: Professional Indemnity for a sum of £2,000,000, Employers Liability for the sum of £10,000,000, and Public & Products Liability for the sum of £5,000,000, Legal Expenses for a sum of £1,000,000.



1. Overview

BEACON is a cloud-hosted safety and critical communications system designed to help organisations protect staff, meet duty-of-care obligations, and respond effectively to unplanned incidents and emergencies.

The service combines a secure web-based management dashboard with mobile applications for staff. It enables organisations to send and receive safety alerts, monitor staff status, manage incidents, and maintain situational awareness in real time. BEACON is suitable for both routine safety operations and unplanned or critical events.

The service is delivered as Software as a Service (SaaS) and does not require customers to install or maintain server infrastructure.

2. Service Features

2.1 Core Functionality

- **Staff Mobile App:** A native mobile application enabling employees to receive alerts, send distress notifications (e.g., panic button), share location information in emergencies, and report incidents directly to the organisation.
- **Operations Dashboard:** A central web-based dashboard for administrators to view real-time status of staff, track locations, initiate advisories, and coordinate responses.
- **Messages:** Secure, real-time and two-way messaging directly between staff and your security team.
- **Geolocation:** Optional geolocation services to enhance situational awareness and aid in coordinating responses, subject to user opt-in.
- **Incident Reporting:** Tools for users to report safety risks, hazards, or other concerns via structured forms within the app.
- **Communications Tools:** Structured messaging and alerting capabilities to disseminate information to defined user groups swiftly during an incident or routine safety communication.
- **Contacts:** Limit panic and increase response times by ensuring staff have the right contact information based upon their location.
- **Convoy:** The optional ability to closely monitor critical and high value convoy movements comprised of vehicles and staff.
- **Panic Button:** Staff can instantly raise and alert and request immediate assistance with a single button
- **Staff Headcount & Status:** Capability to account for staff safety by tracking check-ins and statuses ('OK', 'Not OK'), particularly useful in crisis scenarios.
- **Advisories:** Provide real-time targeted situational information based on your workforce's current location.

2.2 Integrations (subject to availability)

- **Third-party integrations:**
Potential integration with SMS, satellite systems, identity providers, and vehicle tracking for enhanced functionality and existing investments.

3. Data Backup, Restore, and Disaster Recovery

3.1 Data Backup

- Customer data is backed up automatically on a regular basis.
- Backups are encrypted and stored securely in line with industry best practices.
- Multiple backup copies are retained to protect against data corruption or accidental deletion.

3.2 Data Restore

- Data can be restored in the event of system failure, data corruption, or accidental loss.
- Restore processes are managed by the supplier and prioritised according to incident severity.

3.3 Disaster Recovery

- The service is designed for high availability using resilient cloud infrastructure.
- Disaster recovery procedures are in place to restore service in the event of a major incident.
- Business continuity and disaster recovery plans are maintained and tested periodically to ensure service resilience.

4. Onboarding & Offboarding

4.1 Onboarding

The supplier provides onboarding support which may include:

- Initial sessions to understand organisational requirements
- Initial service configuration and tenant setup
- User account creation and role assignment
- Guidance on Staff Mobile App deployment
- Administrator training and documentation
- Assistance with planning pilot and full rollout phases
- Training is delivered using a Train the Trainer approach.

4.2 Offboarding

When the service ends:

- Offboarding is managed in a controlled manner to ensure continuity, auditability, and compliance with data protection obligations.
- Access to the service will be terminated following contract end.
- Data export: where applicable customers can request a copy of their data in an XLXS format.
- Customer data will be securely deleted after an agreed retention period, in line with contractual and legal requirements.

- Customers retain ownership of their data.
- Data access is available for a defined period after contract termination for offboarding up to a maximum of 30-days.
- Secure deletion is performed after the agreed exit process is complete.

5. Service Constraints

5.1 Maintenance Windows

“Planned Maintenance” means any pre-planned maintenance of any infrastructure relating to the Services. CIS will provide the customer with **at least 72 hours** advance notice of any such planned maintenance, the details of which will be discussed and agreed in advance.

“Emergency Maintenance” means any emergency maintenance of any of the infrastructure relating to the Services. Whenever possible, CIS will provide the customer with any details shortly before performing the maintenance.

5.2 Maintenance Management

- Planned maintenance is communicated to customers in advance.
- Emergency maintenance is performed only where necessary to maintain service integrity or security.
- The supplier monitors service availability and responds to outages according to incident severity.
- Customers are informed of significant service disruptions and resolution progress.

5.3 Customisation

We have designed BEACON to be flexible; the service is configurable but not bespoke. There are numerous customisable options available to the customer which include but are not limited to users, roles, alerts, and workflows within defined system parameters.

5.4 Connectivity

Internet connectivity is required all features except for a subset of Staff Mobile App features where defined.

5.5 Integration

Integration with third-party systems is subject to technical feasibility and resource availability.

6. Service Levels

6.1 Availability

Target service availability of **99.8%**. This includes:

- Any unexpected outages of system failures
- Any planned outages (i.e. system updates)
- Any downstream outages.

6.2 Performance

- All connectivity is subject to network conditions.
- Emails, push notifications and SMS rely on external services (using public networks) and therefore are delivered on a best effort basis and subject to recipient device configurations.
- Operations Dashboard updates reflect live or near-live system status.

6.3 Support hours

Standard Support:

- Core hours: Monday to Friday, 09:00–17:00 UK time, excluding UK public holidays and up to 10 additional dates.
- Reduced support outside of core hours is provided on a best-efforts basis.
- Support services are provided exclusively to the customer's designated support contacts. Support will not accept requests from, or engage directly with, end users.
- Designated support contacts must be formally nominated by the customer in writing. These contacts will be provided with direct email addresses, and an out-of-hours contact number.

7. After Sales Support

After-sales support during the length of a contract includes:

- Ongoing technical support and issue resolution
- Access to service documentation and guidance
- Software updates and feature enhancements
- Advice on best practice use of the system

Support is primarily provided through email, though telephone support is also available.

8. Technical Requirements

Access to BEACON is via a modern Internet enabled device with a web browser. No specialist hardware is required.

8.1 Minimum system requirements (Operations Dashboard)

- Laptop or desktop computer device with Internet access
- Modern web browser (standards-compliant, vendor-supported)
- Additional web browser permissions (audio).
- Optional integration with third-party systems via APIs, subject to agreement

8.2 Minimum system requirements (Staff Mobile App)

- Vendor-supported smartphone (iOS or Android) on a compatible OS
- Internet connectivity (Wi-Fi or mobile data)
- Requires additional device permissions enabled (geolocation and push notifications).

9. Hosting Options

- The service is hosted on secure, cloud-based infrastructure.
- Data is hosted in geographically resilient data centres.
- Hosting locations comply with applicable UK data protection requirements.
- Further hosting options are possible upon request.

10. Security

BEACON is designed with security at its core:

- **Access control:** Role-based access for administrators and users
- **Encryption:** Data encrypted in transit and at rest
- **Authentication:** Secure user authentication mechanisms
- **Monitoring:** Continuous monitoring for security events
- **Compliance:** Operates in line with UK GDPR and relevant data protection legislation

Regular updates and security patches are applied to protect the system from emerging threats.

11. Termination of Contract

The supply of Services may be terminated at the end of the contract (if not renewed or extension agreed) or by either party by notice in writing to the other with a minimum of 30 days' notice.

For full details, please refer to the Terms and Conditions document.