

boomAlert Limited
G-cloud 15 Service Definition

Version	1.0
Date	05/01/2026

Contents

1 Company 6

2 Overview 6

3 Services 6

3.1 boomAlert – Incident and Event Alerting 6

Features 6

Uses 6

Benefits 7

3.2 boomCast – Broadcast Messaging 7

Features 7

Uses 7

Benefits 8

3.3 boomMail – Email-2-SMS and Email-2-Voice Messaging 8

Features 8

Uses 9

Benefits 9

4 Approach to Information Assurance 11

4.1 Overview 11

Accreditations and Standards 11

4.2 Information Security Management System (ISMS) 11

Security Controls 11

Incident Management and Business Continuity 12

Data Protection and Privacy 12

Supplier and Shared Responsibility Model 12

Policy Management and Assurance 12

5 Business Continuity Management and Disaster Recovery Provision 13

5.1 Business Continuity Management 13

5.2 Service Resilience and Architecture 13

5.3 Backup and Data Recovery 14

5.4 Monitoring and Capacity Management 14

5.5 Change and Maintenance Resilience 15

5.6 Disaster Recovery 15

5.7 Testing and Continuous Improvement 15

5.8 Buyer Assurance 15

6 Securing the services 16
6.1 Network security 16
6.2 Cloud and platform security 16
6.3 Application security 17
6.4 Malware prevention 17
6.5 Security and vulnerability testing 17
6.6 Securing data 18
Cryptographic controls 18
Data in transit 18
Data at rest and backups 18
Databases 18
6.7 Access controls 18
Internal access controls 18
Customer access controls 18
6.8 Staff recruitment and training 19
6.9 Data retention and legislative compliance 19
7 Customer On-Boarding & Off-Boarding 19
7.1 On-Boarding 19
7.2 Off-Boarding 20
8 Service Management 20
8.1 Background and Overview 20
8.2 Operational Services 21
Account administration 21
Reporting 21
8.3 Training services 21
8.4 Service Constraints and Maintenance 21
Planned Maintenance 21
Unplanned Maintenance 21
Emergency Maintenance 22
8.5 Operational service support 22
Incident Priority Levels 22
8.6 Support packages 22
8.7 SLA penalties and service credits 23
8.8 Account Management Service 23

Account Management Responsibilities 23
Service Reviews and Reporting 24
Ordering and Invoicing 24
9 Customer requirements & Technical Pre-requisites 24
9.1 Customer requirements 24
9.2 Technical pre-requisites 24
User Devices and Access 24
Network and Security 25
Authentication and Identity (where applicable) 25
Customer Responsibilities 25
9.3 Service Constraints 25
Scope of Services 25
Availability and Maintenance 25
Performance and Usage 25
Dependencies and Third-Party Services 26
Data and Integration Constraints 26
Security and Compliance 26
Appendix A – boomAlert Functional Specification 27
1 Overview 27
2 Functionality 27
2.1 Access 27
2.2 Messaging solutions 27
2.3 Messaging features 27
2.4 Administrative functions 28
2.5 Project builder Functions 28
2.6 Remote Activation Functions 29
2.7 Reporting & Audit 29
Appendix B – Functional Specification for boomCast Broadcast Messaging 30
1 Access 30
2 Communications Capability 30
2.1 Communication Channels 30
2.2 Messaging Solutions 30
2.3 Message delivery features 30
3 Interface Capability 30

3.1 Broadcast Builder Features 30
3.2 Remote Broadcasting Features 31
External recipient data 31
Message variable extraction 31
Defer activation 32
Secure requests 32
Authenticate requests 32
Prevent duplicate requests 32
3.3 Inbound Messaging Features 32
Inbound Campaign Manager 32
3.4 System Administration Features 32
User management 32
Stored Contact data 32
Group management 33
Library 33
Organisation Settings 33
System Settings 33
3.5 System Reporting Features 33
Dashboard 33
Message Hub 33
Transaction Reporting 34
Appendix C – Functional Specification for Email-2-SMS & Email-2-Voice Messaging 36
1 Overview 36
2 Access 36
3 Communication Channels 36
3.1 Messaging Solutions 36
3.2 Messaging features 36
3.3 Service management 37
4 Reporting 37
4.1 Dashboard View 37
4.2 Transaction Reporting 37

1 Company

Boomalert Ltd has built a strong reputation, delivering broadcast and incident communication solutions to a range of international clients from both the private and public sectors. We are a specialist in digital communications with almost 20 years' experience and fully focused on delivering high quality 1-way, 2-way and 'Intelligent 2-way' messaging across a range of messaging channels. We have built a suite of solutions that serve an organisation's end-to-end communication requirements, delivering the opportunity to extend engagement through choice, increase operational efficiency by driving automation, and improving customer satisfaction by enabling frictionless stakeholder engagements.

---

2 Overview

boomAlert Limited provides access to a SaaS solution that delivers the following communication tools:

- boomAlert – Automation of incident and event communications
- boomCast – Broadcast messaging from a dynamic, feature rich user interface
- boomMail – Email-2-SMS and Email-2-Voice messaging.

---

3 Services

3.1 boomAlert – Incident and Event Alerting

boomAlert automates the end-to-end management of critical incident communications. It does this by allowing customers to build customised communication workflows with the inherent ability to automatically escalate incident communications across multiple messaging channels, or by contacts. It integrates easily with existing systems so that when a critical event happens, Boomalert is automatically triggered to distribute communications to those that need to know in real-time.

Features

- Customise communication workflows for your different critical events
- Access to multiple communication channels (SMS, Email, voice, and mobile app)
- Integrate with existing systems to implement event triggered workflows
- Automate escalation across different messaging channels to non-responders
- Hunt for acknowledgements by escalating across contacts or groups of contacts
- Count responses for processes requiring quota fulfilment
- Use fully Interactive messaging to engage with responders
- Issue updates during an incident containing real-time incident MI
- Access Incident dashboard to track live incident process

Uses

- IT alerting – Push monitoring alerts to Boomalert to automate communications to engineers

- Weather alerts – Activate Met Office weather alerts and distribute to contacts in affected regions based on severity
- Business continuity – Co-ordinate communications with staff and stakeholders during different BC scenarios
- Lone working – Maintain constant liaison with lone workers and escalate where contact lost
- Product withdrawal – Manage communications with shop floor, PR, legal etc from a single platform to provide a timely and cohesive response

Benefits

- Minimise the impact of an incident by providing an instant response through targeted communications
- Reduce operating costs and improve productivity by automating incident communications
- Improve efficiency of incident management by ensuring the right person has access to the right information exactly when they need it
- Maintain compliance with SLAs by reducing incident resolution times and keeping stakeholders informed
- Fulfil duty of care compliance by adopting an end-to-end solution for lone working
- Improve productivity by issuing pre-emptive weather warnings to mobile staff

A detailed functional specification for boomAlert is available to access at Appendix A

3.2 boomCast – Broadcast Messaging

Our broadcast messaging solution enables delivery of 1-Way and 2-Way broadcast messaging across a range of messaging channels**.** An intuitive interface makes it easy to create bulk broadcasts for instant communication with a widespread audience, helping to reduce the administrative burden, increase operational capacity and drive productivity. Using patented ‘Intelligent Messaging’ for 2-Way broadcasts, automatically creates unique conversation threads with each recipient based on subject matter, allowing system users to easily continue those conversations via a ‘Chat’ feature.

Features

- Access to 1-way and 2-way broadcast messaging
- Replies are automatically matched to the originating campaign using Intelligent 2-way messaging
- Multi-channel messaging over SMS, email, voice and mobile app
- Interactive ‘Chat’ messaging
- Inbound messaging campaigns using SMS short codes and long numbers
- Inbox for all inbound and reply messages
- Scheduled messaging campaigns on ad-hoc or recurring basis
- Global messaging delivery and international messaging using local SMS numbers
- User access controls using roles and permissions to allocate access to systems functions and contact data as required

Uses

- Mass broadcast messaging - announcements, notifications or alerts

- Marketing & promotions – real-time offers, product launch, drive opt-ins, customer feedback
- Transactional messaging – Order confirmations and collections, 2-Factor Authentication, alerts and notifications
- Real-time support using ‘Chat’ – problem solving, customer updates
- End user initiated engagement – customer enquiries, support requests, appointment requests, reporting events (e.g. suspicious behaviour, public hazards, traffic updates etc)
- Scheduled reminders – appointments & meetings, service expiration, renewals,

Benefits

- Extend engagement with end users using Intelligent 2-way messaging
- Reduce operating costs by removing manual communication processes
- Extend reach using multiple communication channels
- Improve customer satisfaction by providing alternative channels of engagement
- Improve service continuity using automated renewal alerts
- Reduce cost of DNAs using automated reminders (appointments, reservations etc)

A full specification for Broadcast Messaging is available in Appendix B.

3.3 boomMail – Email-2-SMS and Email-2-Voice Messaging

Boomerang’s Email-to-SMS and Email-to-Voice services allow organisations to send 1-Way or conversational SMS and voice messages directly from a local email client. Using 'Intelligent' messaging, 2-way conversations are managed automatically, with communication threads grouped by subject rather than time. This ensures that users can easily maintain and manage separate conversations in their email inbox. As all outbound messages and associated responses are recorded, corporate governance and regulatory compliance are maintained.

Features

- **Email-to-SMS and Email-to-Voice Conversion** - Sends SMS or text-to-speech voice messages directly from an email client.
- **1-Way, 2-Way, and Conversational Messaging Support** - Enables outbound-only messaging or full conversational threads with replies returned via email.
- **Secure Access Controls** - Restricts service access by authorised email domains, individual email addresses, IP addresses, or mail servers.
- **SPF-Based Anti-Spoofing Protection** - Prevents email spoofing by validating sender IP addresses against SPF records.
- **Fixed or Dynamic SMS Originator Options** - Allows configuration of alpha originators for SMS, including fixed originator support.
- **Message Management Tools** - Includes character limits, message disclaimers, and signature management to control outbound content.
- **Delivery Status Notifications** - Provides email alerts for failed or undeliverable messages returned by network operators.
- **Social Hours Scheduling** - Controls when messages are sent to ensure delivery only during approved time windows.

- **Advanced Reporting and Dashboard** - Offers real-time dashboards and customizable transaction reports with graphical and tabular views.

Uses

- **Critical Alerts and Notifications** - Send urgent SMS or voice alerts (e.g., system outages, safety incidents, weather warnings) directly from email to ensure rapid delivery to mobile devices.
- **Appointment Reminders** - Automatically send SMS or voice reminders for medical, service, or business appointments to reduce no-shows.
- **Incident and Escalation Management** - Enable IT or operations teams to escalate incidents via SMS or voice calls when email alone is insufficient, with replies routed back to email.
- **Customer Service and Support Communications** - Use 2-way or conversational messaging to communicate with customers via SMS while managing conversations centrally through email.
- **On-Call Staff and Workforce Notifications** - Notify on-call engineers, field workers, or emergency response teams using SMS or voice when immediate action is required.
- **Service Status and Maintenance Updates** - Inform customers or staff about planned maintenance windows, service disruptions, or resolution updates.
- **Compliance and Regulatory Notifications** - Distribute mandatory compliance messages, policy updates, or regulatory alerts with delivery tracking and audit reporting.
- **Internal Communications and HR Messaging** - Share internal announcements, shift changes, or urgent HR notices with employees who may not have regular email access.

Benefits

- **No New Software Required** - Users can send SMS and voice messages directly from their existing email clients.
- **Faster and Simpler Communication** - Enables rapid outreach to mobile users without complex integrations or APIs.
- **Improved Engagement Through Two-Way Messaging** - Supports conversational messaging, allowing recipients to reply and continue interactions via email.
- **Enhanced Security and Compliance** - Strong access controls, SPF validation, and secure data handling reduce the risk of unauthorised use.
- **Global Reach from a Single Platform** - Communicate with recipients worldwide using SMS or voice without managing multiple providers.
- **Consistent Brand Presentation** - Custom originators, signatures, and disclaimers ensure messages align with brand and compliance standards.
- **Reduced Messaging Errors** - Character limits and validation prevent messages from being sent incorrectly or incompletely.
- **Greater Control Over Message Timing** - Social Hours help avoid sending messages outside acceptable or regulatory-approved timeframes.
- **Operational Visibility and Accountability** - Delivery status notifications and detailed reporting improve traceability and issue resolution.

- **Actionable Insights and Performance Tracking** - Comprehensive reporting enables monitoring of usage, costs, delivery success, and recipient engagement.

A full specification for Email-2-SMS / Voice Messaging is available in Appendix C.

---

4 Approach to Information Assurance

4.1 Overview

The organisation operates a comprehensive Information Security Management System (ISMS) that governs the management and protection of customer information and service data. The ISMS is aligned to recognised international standards and UK government guidance and is subject to ongoing review and continuous improvement.

Accreditations and Standards

The organisation holds the following current certifications and independent assurances:

- ISO/IEC 27001:2022 – Information Security Management
- Cyber Essentials and Cyber Essentials Plus
- Financial Services Qualification System (FSQS) – Stage 3 Approved Supplier

In addition, the organisation aligns its security and operational practices with the following recognised standards and principles:

- ISO/IEC 22301 – Business Continuity Management
- ISO 9001 – Quality Management
- ISO/IEC 27701 – Privacy Information Management
- NCSC Cloud Security Principles

4.2 Information Security Management System (ISMS)

The ISMS applies across the organisation, its staff, the cloud services offered, and relevant supply chain activities that process or may access customer data. It includes a documented statement of applicability, defined security objectives, and a risk-based control framework aligned to ISO/IEC 27002:2022.

The ISMS includes:

- Risk assessment and ongoing risk management processes covering customer information and related information assets, based on confidentiality, integrity, and availability (CIA).
- Selection and implementation of proportionate technical and organisational controls aligned with ISO/IEC 27002:2022.
- Defined governance arrangements, including management oversight, performance monitoring, internal audits, independent audits, corrective actions, and continual improvement.
- Regular information security awareness training for all staff, supported by an HR security lifecycle covering recruitment, onboarding, role changes, and leavers.

Security Controls

Security controls are implemented and maintained in line with ISO/IEC 27002:2022 and include organisational, people, physical, and technological controls covering, but not limited to:

- Governance, risk management, and information security policies
- Human resources and personnel security

- Asset management and information classification
- Identity and access management
- Cryptography and key management
- Secure configuration, logging, and monitoring
- Secure development and change management
- Physical and environmental security
- Supplier and third-party security
- Incident management and event reporting
- Business continuity and resilience
- Compliance with legal, regulatory, and contractual requirements

Incident Management and Business Continuity

Information security incidents are managed in accordance with documented procedures, including identification, triage, containment, investigation, and recovery. Personal data breaches are assessed promptly and, where required, reported to the Information Commissioner's Office (ICO) and affected individuals within statutory timescales, in line with UK GDPR and the Data Protection Act 2018.

Business continuity and disaster recovery arrangements are aligned to ISO/IEC 22301 and are designed to support the availability and resilience of the service.

Data Protection and Privacy

The organisation processes personal data in accordance with UK GDPR and the Data Protection Act 2018. Privacy and data protection controls are embedded through:

- Privacy by design and default
- Documented processes for handling Subject Access Requests (SARs)
- Data breach notification and escalation procedures
- Data protection impact assessments (DPIAs) for relevant processing activities

Privacy management controls are aligned to ISO/IEC 27701.

Supplier and Shared Responsibility Model

The organisation operates a shared responsibility model for information security. The organisation is responsible for the security of the service, infrastructure, and operational controls under its management. Customers are responsible for the secure configuration and use of the service in accordance with provided guidance.

All suppliers with access to customer data are subject to due diligence, contractual security obligations, and ongoing assurance proportionate to the risk they present.

Policy Management and Assurance

Information security policies and supporting ISMS documentation are reviewed at least annually or following significant change. A public summary of the Information Security Policy is available on the organisation's website, with additional assurance documentation available to customers upon request under appropriate confidentiality arrangements. Boomerang's Information Security Policy is reviewed at least annually and is available on the company website.

5 Business Continuity Management and Disaster Recovery Provision

Boomerang is responsible for ensuring the resilience and continuity of the Service through a comprehensive Business Continuity and Disaster Recovery (BCDR) framework. This framework is designed to minimise disruption, protect service availability, and ensure rapid recovery from incidents affecting people, processes, technology, or suppliers.

Our approach is aligned with ISO 22301 (Business Continuity Management), ISO 27001, Cyber Essentials Plus, and ITIL best practice, and is reviewed and approved annually by senior management.

5.1 Business Continuity Management

Boomerang maintains formal Business Continuity Plans (BCPs) covering all critical business functions supporting the Service. The objectives of the BCP are to:

- Maintain continuity of critical service operations
- Minimise the impact of disruptive incidents
- Enable a controlled and timely return to business-as-usual
- Safeguard staff, customers, assets, and information

Business continuity planning is underpinned by regular Business Impact Analysis (BIA) and risk assessments to identify critical processes, dependencies, acceptable service loss, and recovery priorities.

BCP arrangements include:

- Defined escalation and incident management procedures
- Clear roles and responsibilities
- Communication plans for customers and stakeholders
- Staff awareness and training
- Consideration of supplier and third-party dependencies
- Annual review and approval by the CEO and Operations Director

Plans are maintained to reflect changes in business operations, technology, or risk profile.

5.2 Service Resilience and Architecture

The Service is architected to **eliminate single points of failure** and provide high availability across infrastructure, platform, and application layers.

Infrastructure and Hosting

- The Service operates across multiple UK-based data centres with real-time data replication between geographically separated locations.
- Automatic multi-site failover is in place, enabling immediate service continuity in the event of infrastructure or network failure.
- All data centres meet recognised industry security and resilience standards.

Cloud Platform

- The Service is delivered on a clustered, cloud-based platform using VMware and Kubernetes.
- The platform supports automatic scaling, ensuring resilience during demand spikes.
- Designed to achieve 99.99% service availability.

Network Resilience

- Redundant, carrier-diverse network connections are in place at all internet-facing edges.
- Multiple high-capacity connections across diverse UK network providers ensure resilience and performance.
- DDoS protection, intrusion detection, and continuous network monitoring are implemented.

Application Resilience

- Services are deployed across multiple instances with load balancing.
- Modular architecture allows individual components to scale independently.
- Multiple messaging suppliers and queues are used to ensure continuity across communication channels.
- Real-time rollback is supported via snapshot-based recovery.

5.3 Backup and Data Recovery

Rigorous back up processes have been implemented to safeguard data.

- Full daily backups are taken and stored off-site.
- Hourly checkpoints are maintained on a rolling 30-day basis.
- Backups are retained for 365 days.
- All backups are verified and regularly tested to ensure successful restoration.
- Data is replicated to secondary storage nodes to maintain availability and integrity.

5.4 Monitoring and Capacity Management

Comprehensive, real-time monitoring is implemented across the Service using industry-standard tooling. This includes monitoring of:

- Service availability and performance
- Infrastructure health (CPU, memory, storage, databases)
- Network traffic and anomalies
- Supplier service performance
- Transactional throughput and messaging success rates

Threshold-based alerts trigger proactive incident response. Capacity and performance metrics are reviewed regularly to ensure the Service continues to meet customer demand and service levels. The platform can be scaled without disruption to live services.

5.5 Change and Maintenance Resilience

Boomerang applies a structured change management process to control modifications to systems, configurations, software and infrastructure.

- All changes are managed through a formal change management process.
- Changes are risk-assessed, approved, and tested prior to deployment.
- Testing is conducted in environments consistent with production.
- Maintenance and updates are performed out of hours where possible, with rollback procedures in place.
- Customers are notified in advance of planned changes in line with support arrangements.

5.6 Disaster Recovery

Boomerang maintains a detailed Disaster Recovery Plan to restore services quickly following a major incident.

- Recovery Time Objective (RTO): 30 minutes
- Recovery Point Objective (RPO): no more than one hour
- Real-time automated failover across multiple data centres.
- Backup restoration procedures tested routinely.
- Incident communication plans ensuring rapid and accurate notifications to affected stakeholders.
- Regular DR exercises, including technical failover and tabletop scenarios, with results logged and improvement actions tracked.

5.7 Testing and Continuous Improvement

Boomerang conducts a structured programme of testing and continuous improvement to ensure that Business Continuity and Disaster Recovery arrangements remain effective, up to date, and capable of meeting service commitments. This includes:

- Business Continuity and Disaster Recovery plans are tested at least quarterly, with different elements tested to ensure full annual coverage.
- Testing includes tabletop exercises and technical failover scenarios.
- Test outcomes are formally recorded, reviewed by senior management, and tracked to closure.
- Lessons learned are used to drive continual improvement of resilience controls.

5.8 Buyer Assurance

This resilience and business continuity approach ensures that public sector buyers receive a highly available, secure, and recoverable service, with clearly defined recovery objectives, tested controls, and governance aligned to recognised international standards.

6 Securing the services

The services are designed and operated in accordance with recognised information security standards and best practice, including ISO/IEC 27001, UK GDPR, and the NCSC Cloud Security Principles. Security controls are implemented using a defence-in-depth approach to protect data, systems, and users throughout the service lifecycle.

6.1 Network security

Network security controls are implemented to protect service boundaries and internal network segments in line with NCSC Cloud Security Principle 1 (Network Security).

Firewalls and other boundary protection devices are deployed at the network perimeter and between key internal network zones. These devices enforce traffic flow policies using access control lists (ACLs) and rulesets that restrict communications to authorised services, ports, and protocols only.

The network is logically segmented to separate web, application, database, and audit logging tiers, reducing the impact of any potential compromise and limiting lateral movement.

Automated monitoring systems are used to monitor network traffic, system availability, and security events. These systems detect unusual or unauthorised activity, including abnormal traffic patterns, port scanning, and intrusion attempts. Alerts are generated where predefined thresholds are exceeded and are handled in accordance with the incident management process.

6.2 Cloud and platform security

The service has been designed and implemented in accordance with the NCSC Cloud Security Principles.

Administrative access to the platform is protected using encrypted VPN connectivity and is restricted by firewall rules and access control lists. Access is granted only to authorised personnel and is subject to formal change control, approval, and regular review.

External access to the platform follows a layered security approach:

- Inbound connections are filtered by external firewall controls
- Approved traffic is further validated by internal firewall systems
- User access is granted only following successful authentication and authorisation

Network-level controls are complemented by identity-based access controls to ensure that access decisions are not based solely on IP address.

The platform architecture is tiered (web, application, database, and logging), allowing access to be restricted to individual components as required. Access permissions, including elevated (Sudo) privileges, are granted on the basis of least privilege and are reviewed regularly.

Independent external security scans and penetration testing are conducted to validate the effectiveness of platform security controls.

6.3 Application security

The service uses a modular application architecture, with components logically separated and secured independently. Communication between components is protected using encrypted channels.

All service access points, including web interfaces and API endpoints, are protected using **TLS (HTTPS)** with industry-standard cipher suites to protect data in transit.

Security is embedded throughout the software development lifecycle in line with NCSC Cloud Security Principle 7 (Secure Development). A Secure Development Policy ensures that:

- Access to development environments is restricted and granted on a need-to-know basis
- Development and test environments are appropriately secured and segregated from production
- Security requirements are considered during design and planning
- Code is developed in line with recognised best practices (such as OWASP guidance) and stored in secure version control repositories
- Security testing forms part of the testing and release process

6.4 Malware prevention

Malware protection controls are implemented across the service infrastructure.

Automated malware scanning is deployed on servers and supporting systems, using regularly updated signatures and detection mechanisms. Monitoring tools are used to identify potentially malicious activity, including indicators of compromise or unauthorised changes.

Operational staff are trained to recognise and respond to suspected malware incidents. Any detected malware is isolated and quarantined, and alerts are raised internally for investigation and remediation in line with the incident management process.

6.5 Security and vulnerability testing

Security testing is carried out regularly to ensure that the service remains protected against known vulnerabilities and emerging threats, in line with NCSC Cloud Security Principle 4 (Monitoring and Auditing).

This includes:

- Independent penetration testing of the service infrastructure at least annually
- Regular vulnerability scanning of all service components
- Web application security testing aligned to recognised standards such as the OWASP Top 10
- Continuous monitoring for common vulnerabilities and misconfigurations

Identified vulnerabilities are risk-assessed, prioritised based on severity, and remediated within defined timescales.

6.6 Securing data

Cryptographic controls

Cryptographic controls are used to protect data at rest and in transit, in line with NCSC Cloud Security Principle 5 (Data Protection).

Data in transit

All access to the service via web interfaces or APIs is protected using TLS encryption. This applies to desktop and mobile access.

Data at rest and backups

Backup data is encrypted using AES-256 encryption. Encryption keys are securely generated, stored, and managed using controlled key management processes, with access restricted to authorised personnel only.

When storage media reaches the end of its useful life, data is securely destroyed in accordance with NIST SP 800-88 (Guidelines for Media Sanitization) to prevent unauthorised data recovery.

Databases

Sensitive data stored within databases is protected using encryption mechanisms provided by the database platform. Encryption is applied to protect data throughout its lifecycle.

6.7 Access controls

Access to systems and data is governed by formal access control policies aligned to NCSC Cloud Security Principle 6 (Identity and Authentication).

Internal access controls

- Access to systems processing customer data is granted on the basis of least privilege
- All access is formally authorised and subject to regular review
- Each user is assigned a unique user ID
- Security-relevant actions are logged with date and time stamps
- Asset owners are responsible for reviewing access rights and ensuring they remain appropriate

Audit logs are protected from unauthorised modification and are reviewed to support security monitoring and investigation.

Customer access controls

Customer access to the service is protected by authentication controls, password management, and optional multi-factor authentication. Role-based access controls allow customers to define permissions aligned to job roles and responsibilities.

Customers can control access to personal and transactional data on a need-to-know basis, and data can be anonymised where required.

Customers retain control of the data they submit to the service and can modify or delete it at any time. Customer data is deleted following the end of a trial or contract period in accordance with agreed retention policies. Access to customer data by service staff is

restricted and occurs only at the customer's request or where required to investigate service-related issues.

6.8 Staff recruitment and training

Personnel security controls are implemented in line with NCSC Cloud Security Principle 8 (Personnel Security).

Appropriate pre-employment screening and checks are carried out for employees and contractors. All personnel are required to comply with the organisation's information security policies as part of their contractual obligations.

Information security training is provided at regular intervals and is recorded as part of each individual's development plan. Updates on emerging threats, security issues, and regulatory requirements are communicated to staff as needed.

Compliance with security policies and procedures is verified through regular internal and external audits.

6.9 Data retention and legislative compliance

Data flows involving personal data have been mapped across the organisation. Data retention policies are implemented to ensure that data is retained only for as long as necessary and in accordance with the purpose for which it was collected.

The service is operated in compliance with applicable data protection legislation, including UK GDPR and the Data Protection Act 2018.

Procedures are in place to identify, manage, and report personal data breaches in accordance with regulatory requirements and contractual obligations.

---

7 Customer On-Boarding & Off-Boarding

7.1 On-Boarding

Our on-boarding process is designed to ensure customers can begin using the service quickly, securely, and with minimal disruption.

Once an order is confirmed, we will work with the customer to agree an implementation plan covering timescales, responsibilities, and any service-specific configuration requirements. A named point of contact will be provided for the duration of the on-boarding process.

On-boarding activities may include:

- Account creation and user access setup
- Configuration of the service in line with customer requirements
- Integration with customer systems, where applicable
- Security and access controls aligned to customer policies
- Data migration or initial data upload (if required and agreed)
- User guidance and onboarding documentation

- Training

The service is delivered using standardised processes to minimise risk and ensure consistency. Any customer dependencies or prerequisites will be clearly communicated in advance. Where applicable, testing or validation will be completed before the service is made live.

There is no additional charge for standard on-boarding unless otherwise stated in the pricing document.

7.2 Off-Boarding

Our off-boarding process ensures that customers can exit the service in a controlled, secure, and transparent manner at the end of the contract or upon termination.

Upon receiving notice to off-board, we will agree an exit plan with the customer, including timelines and any specific requirements. Off-boarding activities may include:

- Secure extraction and return of customer data in a commonly used format
- Confirmation of data ownership and transfer arrangements
- Deactivation of user accounts and access credentials
- Removal of customer-specific configurations
- Secure deletion of customer data from our systems in line with our data retention and destruction policies
- Confirmation of service termination

Data will be handled in accordance with applicable data protection legislation, including the UK GDPR. Data deletion will be completed within agreed timescales following contract termination, unless otherwise required by law.

Where requested, we will provide reasonable assistance to support transition to an alternative supplier. Any additional off-boarding support beyond standard activities may be subject to additional charges, which will be agreed in advance.

---

8 Service Management

8.1 Background and Overview

Boomerang provides a cloud-hosted Software as a Service (SaaS) solution designed for use by UK public sector organisations. The services are accessed via a secure web-based user interface and/or Application Programming Interfaces (APIs). No local software installation or downloads are required*.

The service has been designed to operate in accordance with relevant UK legislation and government policy, including environmental and sustainability objectives. Ongoing service management activities are delivered in line with G-Cloud 15 requirements.

*Excludes Plug-In for Dynamics 365

8.2 Operational Services

Account administration

Boomerang will provide a user interface or managed service for the customer which will include the ability to achieve the following:

- Provision and management of account configuration and settings
- Provision of other service users and management of access
- Addition of services, products, or features
- Amendment of existing service, product, or feature selections
- Access to transactional messaging data reports

Reporting

Customers have access to transactional and analytical reporting data relating to their use of the service via the user interface. Reporting access is controlled by user permissions. Reports can be viewed online and exported in standard formats.

8.3 Training services

Training is provided as part of the onboarding process and is delivered remotely (telephone or online) unless otherwise agreed. Training sessions are arranged by the customer's Account Manager in collaboration with the customer.

As standard, onboarding training covers:

- Account configuration and administration
- Service overview and provisioning
- Use of the user interface
- Reporting
- Billing
- Support processes

Additional or refresher training can be provided on request and may be chargeable. Training can be delivered in an accessible format where required.

8.4 Service Constraints and Maintenance

Maintenance activities are categorised as follows:

Planned Maintenance

Planned maintenance includes scheduled activities required to maintain service security, stability, and performance. Where possible, planned maintenance is scheduled to minimise disruption.

- Customers receive a minimum of **5 working days' notice**
- Notifications are issued to designated contacts before and after maintenance
- Planned maintenance is excluded from availability calculations

Unplanned Maintenance

Unplanned maintenance may be required to prevent or mitigate service degradation or potential service disruption. Where possible, customers will be informed during the activity.

Emergency Maintenance

Emergency maintenance is carried out to address critical issues affecting service availability, performance, or security. Due to the urgent nature of such work, advance notice may not be possible.

8.5 Operational service support

Operational support includes incident management and service requests.

Support requests are logged and tracked using Boomerang's technical support case management system and may be raised by authorised customer contacts or by Boomerang on the customer's behalf.

Incident Priority Levels

Support incidents are prioritised as follows:

- **Priority 1 (High):** Complete loss of service or a critical issue with significant business impact
- **Priority 2 (Medium):** Partial loss of service or significant degradation of functionality
- **Priority 3 (Low):** Non-critical issues, general queries, or service requests

Service requests may include "how-to" queries, billing enquiries, and service change requests.

8.6 Support packages

Two support packages are available: **Standard Support** and **Premium Support**. Standard Support is included as part of the base service. Premium Support is optional and chargeable.

Premium Support may be provided on an annual term. Alternative terms may be agreed with public sector customers

Support element	Standard Support	Premium Support*
Support availability		
Support times	9am-6pm, Mon-Fri (UK)	24/7/365
Support channel	Email	Email, Telephone
System availability		
Target availability	No commitments	99.50%
Issue response times		
Severity level 1	Within 1 working day	1 hour
Severity level 2	Within 2 working days	1 hour
Severity level 3	Within 3 working days	1 hour
Service Restoration Target		
Severity level 1	Best endeavours	3 hours
Severity level 2	Best endeavours	12 hours

Severity level 3	Best endeavours	2 working days
Scheduled Maintenance		
Notice period	Minimum 5 days	Minimum 5 days
Actions per month	No commitments	Maximum of 2
Terms		
Minimum term	N/A	12 months
Subscription Payment Terms	N/A	Annual in advance

*Chargeable as per G-Cloud 15 Price List.

Premium Support may be provided on an annual term. Alternative terms may be agreed with public sector customers.

8.7 SLA penalties and service credits

Customers with Premium Support are eligible for Service Credits where Boomerang fails to meet the monthly System Availability target of **99.50%**.

System Availability is measured on a calendar-month basis and excludes periods of planned maintenance notified in advance.

Where the availability target is not met, the customer may claim a Service Credit equal to 10% of the monthly subscription fee for the affected service (calculated as one twelfth of the annual subscription).

Service Credits:

- Apply only to the service subscription fee
- Do not apply to usage-based charges or third-party costs
- Must be claimed within **30 days** of the end of the affected month

Service Credits are not available where the customer is in material breach of the agreement, including non-payment at the time the outage occurred.

8.8 Account Management Service

Each customer is assigned an Account Manager who acts as the primary point of contact for service management and ongoing engagement.

Account Management Responsibilities

The Account Manager is responsible for:

- Coordinating service onboarding
- Acting as a point of escalation for service-related issues
- Providing regular service reviews and performance updates

The customer is responsible for:

- Nominating appropriate operational, technical, and commercial contacts
- Participating in agreed service review meetings

Service Reviews and Reporting

The standard account management model includes:

- A post-implementation check-in
- Quarterly service review meetings conducted remotely unless otherwise agreed

The Account Manager will provide:

- Meeting notes and agreed actions
- Periodic service performance summaries

There are no contractual SLAs associated with account management activities.

Ordering and Invoicing

Customers may order additional services or features via the user interface or by issuing a purchase order. Invoices are issued electronically in PDF format, provided to designated billing contacts, and can also be accessed from Boomerang the user interface.

The standard billing model is as follows:

- Service subscriptions are charged annually in advance
- Usage-based charges are billed monthly in arrears or deducted from pre-paid credits
- Invoices include a breakdown of usage and associated costs

Alternative billing arrangements may be agreed for public sector customers and documented in the customer agreement.

Billing queries should be submitted in writing within 20 days of the invoice date. Unresolved queries may be escalated in accordance with Boomerang's billing procedures.

There are no contractual SLAs associated with ordering and invoicing activities.

---

9 Customer requirements & Technical Pre-requisites

9.1 Customer requirements

Customer requirements are defined in context within the relevant sections of this document and also in Customer's Obligations' of the 'Terms and Conditions' which defines the consumer's obligations in full. These terms and conditions are also available in the G-Cloud catalogue.

9.2 Technical pre-requisites

To use the service effectively, customers must ensure that the following technical pre-requisites are met:

User Devices and Access

- A modern web browser (latest or previous major release of Google Chrome, Microsoft Edge, Mozilla Firefox, or Apple Safari).
- JavaScript and cookies enabled within the browser.

- A stable internet connection with sufficient bandwidth to support normal service usage.

Network and Security

- Ability to access the service over HTTPS (TCP port 443).
- Customer networks must allow outbound connections to the service's URLs and APIs.
- Any customer-managed firewalls, proxies, or content filters must be configured to permit service traffic.
- For API access (where applicable), customers must support RESTful APIs over HTTPS.

Authentication and Identity (where applicable)

- Customer-managed user accounts, or integration with supported identity providers (e.g. SAML 2.0, OAuth 2.0, or Microsoft Entra ID / Azure AD).
- Customers are responsible for managing user credentials, roles, and access permissions unless otherwise stated.

Customer Responsibilities

- Provisioning and maintenance of end-user devices.
- Management of local network infrastructure.
- Compliance with internal security policies and relevant data protection obligations.
- Timely application of updates to any customer-managed systems that integrate with the service.

9.3 Service Constraints

The following constraints apply to the services:

Scope of Services

- The service is provided as described in the Service Definition. Functionality outside this scope is not included unless agreed via a separate contract.
- Custom development or bespoke configuration is not included unless explicitly stated.

Availability and Maintenance

- The service is designed to be available 24x7, excluding planned maintenance.
- Planned maintenance will be communicated in advance wherever possible and is typically conducted outside UK business hours.
- Emergency maintenance may be required to maintain service security or stability.

Performance and Usage

- Performance may be affected by customer network connectivity, device capability, or third-party dependencies.
- Fair usage policies may apply to prevent excessive or abusive consumption of system resources.
- Any published service limits (e.g. storage, user numbers, API calls) are defined in the service documentation.

Dependencies and Third-Party Services

- The service may rely on third-party components or cloud infrastructure providers.
- The supplier is not responsible for outages or issues caused by failures in customer systems or third-party services outside the supplier's control.

Data and Integration Constraints

- Data import/export is supported only in the formats documented for the service.
- Integrations are limited to supported APIs and interfaces.
- Customers are responsible for the accuracy and legality of data entered into the service.

Security and Compliance

- Customers must not attempt to circumvent service security controls.
- The service must be used in accordance with applicable laws and regulations.
- Any additional compliance requirements beyond those stated in the Service Definition may require separate agreement.

Appendix A – boomAlert Functional Specification

1 Overview

Boomalert is a software application accessed via the Boomerang UI interface, enabling the configuration and activation of automated communication workflows across multiple messaging channels. Workflows can be configured to automatically escalate based on communication channel, individual contacts or by groups of contacts. Responses to outbound communications are processed, allowing the content of a response to automatically trigger different pre-defined workflows can be activated locally, via the user interface, or remotely via SMS, Email and HTTPS. All outbound and inbound message activity is recorded and can be accessed as a report, from the user interface or via email and SMS.

2 Functionality

2.1 Access

A graphical user interface hosted on an SSL secured URL is provided for user access. User access is controlled via secure login and a structured set of permissions, aligned to the system functionality. Remote access is provided to activate a pre-defined workflow, via SMS and Email and over HTTP.

2.2 Messaging solutions

Boomalert supports global messaging over SMS, Email and Voice (delivered as Text-to-Speech) along with the following messaging solutions:

1-Way Messaging via:

- SMS
- Email (reply optional)
- Voice (reply optional)

Intelligent 2-Way messaging via:

- SMS
- Email
- Voice messages
- Voice IVR

2.3 Messaging features

The following features relating to outbound messaging are available:

- Validity* – Provides the ability to set an expiration period against an Intelligent 2-Way message. This determines the period over which a response will be matched to the originating outbound message.
- Open ticket – Matches multiple responses to the same outbound message within the message validity period.

- Social hours – Provides the ability to set the times between which messages will be sent by Boomerang. Messages received by Boomerang between are only processed outside of the designated ‘Social Hours’.
- Priority messaging – Provides the ability to override Social Hours messaging to ensure that a message is sent at all times.
- Localised messaging – Messages are delivered using an originating number that is local to the Recipient’s destination.
- Secure Data – Message content, response content and communication addresses are overwritten.

*Mandatory

2.4 Administrative functions

The Boomalert application supports the following capability that is managed from the user interface:

- **Secure access –** Secure SSL encrypted access with stringent user password criteria and 2-factor authentication. Multiple invalid login attempts trigger a lock on the user account and / or the originating IP address.
- **User management –** Add and edit system users and control access through configurable user roles consisting of a structured permission set.
- **Stored Contact data –** Add single recipients or import bulk recipients directly via the user interface. Supported import functions are: .CSV, Excel and Cut and Paste.
- **System settings** – Manage system default settings relating to:
  - The user interface
  - System contacts
  - Communication channels
  - System Administration
- **Organisation Settings** – Access and edit company information stored in the account, view products in use and configure the security settings across all products.
- **Group management –** Create and edit Groups of system contacts:
  - Manually based on selection of individual recipients
  - Dynamically based on Contacts that match a pre-defined set of criteria associated to the Group.
  - Set the times between which a Group is active, to determine when the recipients in that Group are eligible to receive messages.
- **Project data management** – Group communication workflows and their associated entities into separate system projects.
- **Library** – Create template items that can be re-used when building a project workflow. Once selected in a workflow project, a copy of the library item is created which becomes unique to that project.

2.5 Project builder Functions

Build and store automated communication workflows, including but not limited to:

- Broadcast Alerts – Send staggered or simultaneous notifications via one or more communication channels.

- Escalation Alerts – Escalate communications by communication channel or recipients / distribution groups after a specified period of time across different channels based on:
  - Failure to receive a response from an individual contact
  - Failure to meet a required quota of responses across all recipients
- Fulfilment Alerts – Escalate communications to achieve a designated quota of responses by:
  - Individual Recipients
  - Distribution Groups
- Conversational workflows – Automated interactive workflows, where a recipient's response to one message triggers the next message sent based on response keywords
- Time based Notification and Alerts – Schedule notifications and alerts according to time based milestones as follows:
  - The progress / status of an active workflow project
  - A specified period of time
- Time based actions – Workflow Actions determined by time:
  - Intervals between escalation of communication channels
  - Intervals between workflow escalation to a recipient of distribution group
  - Duration of a workflow / project
  - Wait time for a single response or a specified quota of responses, with actions to escalate a workflow or stop a workflow / Project.

2.6 Remote Activation Functions

To remotely activate a pre-defined Project Users can access:

- **Integrations** – Build APIs connecting Boomalert to third party software applications to trigger projects based on a pre-defined rule set to manage API requests.
- **Triggers** – Create project Triggers that define the criteria via which a project can be activated.
- **Project activation** – Activate communication workflows via the user interface or remotely via SMS and Email or over HTTP(S).

2.7 Reporting & Audit

- Dashboard summary reports. Warnings and notifications generated automatically within the application, based on system activity and an activity stream providing details of key actions taken within the account for auditing.
- Live Incident Reporting Dashboard
  - Provides access to incident status overview and a detailed breakdown of all outbound and inbound communications.
  - Responders are automatically grouped by context
  - Historical incident activity and scheduled activities are recorded.

Appendix B – Functional Specification for boomCast Broadcast Messaging

1 Access

A graphical user interface hosted on an SSL secured URL is provided, to enable the configuration of outbound broadcast campaigns and inbound SMS campaigns. User access is controlled via secure login and a structured set of permissions, aligned to the system functionality.

2 Communications Capability

2.1 Communication Channels

International messaging is supported via:

- SMS
- Voice (delivered as Text-to-Speech)
- Email

2.2 Messaging Solutions

The following messaging solutions are supported:

- 1-Way Messaging via SMS
- 2-Way messaging via SMS, Voice, and Email
- Intelligent 2-Way messaging via SMS and Email (recipient replies are matched to each individual broadcast)
- Conversational messaging via SMS, Email and Voice (conversation threads are created and managed according to subject matter and accessed via ‘Chat’ view)
- Inbound messaging campaigns (receiving end user initiated messages)

2.3 Message delivery features

The following features can be applied to control delivery of messages and message data:

- Social hours – Set the times between which messages will be sent by Boomerang. Messages received by Boomerang are only processed between designated ‘Social Hours’ (e.g. 8am – 8pm)
- Priority messaging – Provides the ability to override Social Hours messaging to ensure that priority messages can be sent when required
- Secure Data – Message content, response content and communication addresses are overwritten to anonymise transactional data
- Localised messaging – 2-way messages are delivered using an originating number that is local to the recipient’s destination (subject to availability of numbers)

3 Interface Capability

3.1 Broadcast Builder Features

Create and store outbound broadcast campaigns, incorporating the following functionality:

- Create a 1-way SMS Broadcast using a customisable originator limited to a maximum of 11 characters.
- Create a 2-way Broadcast over SMS, Email and voice with replies matched to the outbound transaction per recipient
- Create a broadcast using an inbound campaign number as the originator with replies mapped back to the campaign Inbox
- Import recipients and variable data from an Excel file which is inserted into the message content (the imported content replaces the variable token in the message body)
- Short links – Convert long URLs to short URLs with access and security controls and reporting on access to the link
- File sharing – Include short links to stored documents / files within message content
- Schedule broadcasts for delivery on a specific date and time with the option to repeat that Broadcast according to a specified frequency and over a specified period of time.
- Insert variable data into the content of a message based on information associated to contacts stored in the system (e.g. personalising a message by inserting data from the ‘First Name’, and ‘Last Name’ fields)
- Send multi-part (concatenated) messages delivered to the recipient as a single message and use a character /message counter to calculate the number of messages
- Broadcast messages in different languages including support for Unicode character sets
- Save a broadcast as a template which can be reused
- Preview broadcast data prior to sending
- Recipient management:
    - Select stored system contacts
    - Select stored groups (distribution lists)
    - Copy and paste a list of destination addresses (telephone numbers and email addresses)
    - Import contacts from an Excel spreadsheet
    - Pass contacts from an external data source via HTTPS or Email (along with message content or message variables inserted into the broadcast content)
- Push responses returned by recipients to an email address in real-time

3.2 Remote Broadcasting Features

Create broadcast templates that can be activated remotely via HTTPS or Email, enabling the following functionality.

External recipient data

Allows recipient data from an external data source to be passed in the activation request.

Message variable extraction

Create variables that can be extracted from the activation request and the corresponding value associated that variable, is inserted into the template message content (replacing variable tokens inserted in the template message).

Defer activation
Schedule a broadcast to be processed relative to a date / time passed against a specified variable. For example, the variable 'Event Time' could be passed in the activation request with an associated value 10/11/2023 16:00. If the deferred period was set to 24 hours, Boomerang would automatically process the broadcast at 16:00 on 09/11/23, regardless of when the request was submitted to Boomerang.

Secure requests
Requests originating only from recognised email domains or IP addresses will be authenticated.

Authenticate requests
Apply authentication to remote activation requests by notifying designated contacts who must reply to authorise activation.

Prevent duplicate requests
Duplicate requests received within a specified time period will be rejected and relevant contacts notified

3.3 Inbound Messaging Features

Allow end users to initiate engagement with access to the following functionality.

Inbound Campaign Manager
Create inbound messaging campaigns allowing an end user to submit a message to an SMS short code or long number, with options to:

- Use predefined keywords for multiple campaigns on a single number
- Return an automated reply message to an inbound message (customisable per keyword)
- Forward an inbound message to one or more email addresses (customisable per keyword)
- Forward an inbound message to a callBack URL (customisable per keyword)
- Forward an inbound message to all members of a specified system group
- Define a start and end date for the campaign that determines between when inbound messages will be accepted and processed.
- Access inbound messages per campaign and create campaign reports

3.4 System Administration Features

The features listed below enable administrative control of messaging services.

User management
Add and edit system users and control access to system functionality by creating user roles consisting of different permission sets. Limit access to sensitive data to designated users. Enable 2FA access to the software for all users using a one-time passcode.

Stored Contact data
Add individual recipients or import bulk recipients directly via the user interface. Create custom contact fields to capture specific data required for your contacts.

Group management
Create and manage distribution lists containing system contacts. Contacts can be assigned:

- Manually based on selection of individual recipients
- Dynamically based on data contained in contact fields that match a set pre-defined conditions created against a Group. Dynamic grouping automatically includes / excludes contacts that meet / do not meet the conditions associated to a group, to minimise manual administration

Library
Create and manage broadcast templates and logically organise templates using folders. Upload documents and files to the library that are included in broadcasts messaging content using short links.

Organisation Settings
Access and edit company information stored in the account, view products in use and configure the security settings (e.g. 2FA for user access). Activate, create, and manage system departments that control user access to system contacts.

System Settings
Create system defaults and manage settings for:

- Appearance and configuration of the user interface
- Creating and editing bespoke data fields to capture data associated to contacts
- Default system time zone
- Restricting visibility of sensitive data associated to contacts across the system
- Making specified communication channels mandatory when creating or editing contacts
- Default data associated to the available communication channels (e.g. a default email from address or 1-Way SMS originator (these can be overwritten when creating a broadcast)).

3.5 System Reporting Features

The features listed below enable access to analytical and reporting data across the system.

Dashboard
Landing page providing access to widgets containing summary data relating to:

- System configuration progress
- Messaging activity by communication channel and delivery status
- Recent broadcasts
- System contacts and groups
- Inbound campaigns
- System user activity

Message Hub
Repository providing access to messaging data as follows:

- Broadcast history – A record of all previous broadcasts containing:

    - Broadcast title
    - Date / time
    - System user initiating the broadcast
    - Communication channels used
    - Summary of message delivery statuses across all recipients
    - Content of the broadcast
    - Recipient name / communication address
    - Delivery status per recipient and delivery status timestamps
    - Replies received per recipient and reply content (selecting a reply provides access to ‘Chat’ feature containing a conversation history option to send further messages)
- Scheduled Broadcasts – A record of all active scheduled broadcasts containing:
    - Broadcast title
    - Date created
    - System user that scheduled the broadcast
    - Next send date / time
    - Frequency of repetition (if broadcast is set to repeat)
    - Stop action to deactivate the scheduled broadcast
- Inbound Campaigns – A record of all inbound message campaigns containing:
    - Campaign name
    - Status (Active / Inactive)
    - Date created
    - System user that created the campaign
    - Inbound number associated to the campaign
    - Campaign keywords created (if created)
    - Inbound message details
- Inbox – Repository for all inbound messages and broadcast replies containing:
    - End user details (name if stored as a contact and communication address)
    - Date and time received
    - Message content (selecting a reply provides access to ‘Chat’ feature containing a conversation history option to send further messages)
    - Sort by – Read / Unread / Flagged
    - Option to archive inbound message

Transaction Reporting

Reporting tool providing the ability to build customised reports relating to messaging activity and system activity including reporting by:

- Period / Date Range – Predefined selections or custom date range
- Transactions – Number of individual message transactions
- Billable – Number of billable records
- Communication channel
- Message direction (1-Way / 2-Way)
- Inbound messages and replies
- Message delivery status
- Individual recipients
- Users

Reporting data is accessed as either graphical chart or via a tabular view containing the detailed transactional message data relating to the parameters selected.

Appendix C – Functional Specification for Email-2-SMS & Email-2-Voice Messaging

1 Overview

A service that accepts email messages submitted from an email client to a designated Boomerang email address (that includes the recipient's mobile number). The email request is then converted to an SMS or voice message and sent to the number provided in the email address. 1-way and 2-way and conversational messaging are supported and where 2-way or conversational messaging are used, recipient responses are converted back to an email message and sent to the originating email address.

2 Access

The service is accessed from an email client by sending an email message to a designated email address provided by Boomerang. The service will only accept requests originating from an authorised email domain or series of authorised email addresses. It is also possible to restrict access to a mail server address. Spoofing is protected against by using SPF rules which ensure that the IP address used to send an email must match that set in the SPF record.

3 Communication Channels

The service supports global messaging over SMS and Voice (delivered as Text-to-Speech).

3.1 Messaging Solutions

The following messaging solutions are supported:

- 1-Way SMS Messaging – Messages are delivered to the recipient's device with an alpha originator which is set in the Email Subject field. The recipient is unable to reply
- 1-Way Voice Messaging – Messages are delivered via a telephone call with the message content played via text-to-speech
- Conversational messaging – Separate conversational threads are automatically created based on the Email Subject between the service user and the recipient this

3.2 Messaging features

The following features relating to outbound messaging are available:

- **Fixed originator (SMS) –** Use a static dynamic header as the originator for all outbound SMS messages. 2-way messaging is not supported where a fixed originator is used.
- **Message Disclaimer –** Pre-defined, custom content that is appended to all outbound SMS or voice messages.
- **Character Limit –** Messages containing more characters than a pre-defined threshold value set by the customer are not sent, and an error message is returned to the user.
- **Signature Manager** – A pre-defined, custom value that is used to denote the end of a message. Any content located after the specified value is not included in the message.

- **Delivery status notifications –** Provides the option to receive status updates for the messages for which a failed or undeliverable notification is returned by the recipient's network operator. Notifications are sent as an email to the originating user.
- **Social hours** – Provides the ability to set the times between which messages will be sent by Boomerang. Messages received by Boomerang between are only processed outside of the designated 'Social Hours'.
- **Secure Data** – Message content, response content and communication addresses are overwritten.

3.3 Service management

Access to Boomerang's user interface to manage service settings for:

- **Security** – Define system user access by adding individual email addresses (with the option to trigger a welcome email to new users), an email domain, an IP address or a mail server address.
- **User management –** Add and edit system users and control access through configurable user roles consisting of a structured permission set.
- **Outbound messaging** – configuration options relating to the attributes of an outbound message.
- **Service notifications** – Set Email and URL addresses to which unmatched responses can be forwarded.
- **Communication Defaults** - Configure default attributes for SMS and voice communications

4 Reporting

4.1 Dashboard View

Summary reports are provided via widgets in a Dashboard view covering messaging activity, system activity and information relating to the status of your account.

4.2 Transaction Reporting

Reporting tool providing the ability to build customised reports relating to messaging activity and system activity including reporting by:

- Period / Date Range – Predefined selections or custom date range
- Transactions – Number of individual message transactions
- Billable – Number of billable records
- Communication channel
- Message direction (1-Way / 2-Way)
- Inbound messages and replies
- Message delivery status
- Individual recipients

Reporting data is accessed as either graphical chart or via a tabular view containing the detailed transactional message data relating to the parameters selected.