Boomerang Service Definition for G-Cloud 14

Version	1.4
Date	5th April 2024

Contents

1 Company 6

2 Overview 6

3 Document Purpose 6

4 Services 7

4.1 Broadcast Messaging 7

4.2 Workflow Messaging 7

4.3 API Messaging 7

boomAPI 7

4.4 Microsoft Messaging 8

Microsoft Custom Connector 8

Dynamics 365 Messaging Plug-In 8

4.5 Email-to-SMS and Email-to-Voice Messaging 8

5 Approach to Information Assurance 9

6 Business Continuity Management and Disaster Recovery Provision 11

6.1 Infrastructure 11

Multi-site failover 11

Cloud solution 11

Network architecture 12

Service applications 12

6.2 Back-ups 12

6.3 Monitoring 12

Network 13

Platform 13

6.4 Capacity Management 13

6.5 Change Management 14

QA Testing 14

Configuration updates 14

Notification of changes 14

6.6 Disaster Recovery 14

7 Securing the services 15

7.1 Network security 15

7.2 Cloud security 15

7.3 Application security 15

7.4 Malware prevention 16
7.5 Security and vulnerability testing 16
8 Securing data 17
8.1 Cryptographic controls 17
Data stored on back up devices 17
Accessing service applications 17
Database 17
8.2 Access controls 17
Access controls within Boomerang 17
Access controls within services used by customers 18
8.3 Staff recruitment & training 18
8.4 Data retention and legislative compliance 18
9 Customer On-Boarding & Off-Boarding 19
9.1 On-Boarding 19
Trial service 19
Proof of concept (POC) 19
Production services 19
Implementation support and training 19
9.2 Customer off-boarding 20
Termination 20
Service migration 20
10 Service Management 21
10.1 Background and Overview 21
10.2 Operational Services 21
Account administration 21
Reporting 21
10.3 Training services 21
10.4 Service Constraints 21
Planned maintenance 21
Unplanned maintenance 22
Emergency maintenance 22
10.5 Operational service support 22
10.6 Support packages 22
10.7 SLA penalties and service credits 23

10.8 Account Management Service....23
Account Management Overview and Responsibilities....23
Pre-Implementation Account Management....23
Post implementation Account Management....24
Account Management Reporting....24
10.9 Ordering and Invoicing....24
11 Customer requirements & technical pre-requisites....26
11.1 Customer requirements....26
11.2 Technical pre-requisites....26
User Interface....26
APIs....26
Appendix A - Functional specification for Broadcast Messaging....27
Access....27
Communication Channels....27
Messaging Solutions....27
Broadcast Builder Features....27
Remote Broadcasting Features....28
External recipient data....28
Message variable extraction....28
Defer activation....28
Secure requests....28
Authenticate requests....28
Prevent duplicate requests....29
Message delivery features....29
Inbound Messaging Features....29
Inbound Campaign Manager....29
System Administration Features....29
User management....29
Stored Contact data....29
Group management....30
Library....30
Organisation Settings....30
System Settings....30
System Reporting Features....30

Dashboard....30
Message Hub....30
Transaction Reporting....31
Appendix B - Functional specification for Workflow Messaging....33
Communication Channels....33
Messaging Solutions....33
Example Uses....33
Workflow Engine....34
Workflow Components....34
Activation channels....34
Activation functions....34
Broadcast Features....36
Appendix C – Functional Specification for API Messaging....41
boomAPI....41
Appendix D – Functional Specification for Microsoft Messaging....42
Microsoft Custom Connector....42
Dynamics 365 Messaging Plug-In....42
Appendix E – Functional specification for Email-to-SMS and Email-to-Voice Messaging....43
Overview....43
Access....43
Communication Channels....43
Messaging Solutions....43
Messaging features....43
Service management....44
Reporting....44
Dashboard View....44
Transaction Reporting....44

1 Company

Boomerang I-Comms Ltd has built a strong reputation, globally, delivering a digital messaging capability to a wide 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

Boomerang offers a range of messaging solutions via an intuitive user interface and APIs that fulfil a broad range of messaging requirements. Our objective is to help organisations extend automation across customer and stakeholder engagements. Our 'Intelligent' conversation threading technology is unique and patented in over 50 countries and is pivotal to the products and services we deliver to our customers. Fundamentally, it addresses the core problems that have prevented true automation of business communications.

3 Document Purpose

This Service Definition outlines the various messaging services provided by Boomerang and how these services are delivered to customers. The functional specifications for each of the available messaging services offered by Boomerang is set out in the appendices.

4 Services

Our comprehensive range of cutting edge solutions empower organisations to fulfil their communication requirements from a single platform. A detailed specification for each solution is provided in the appendices to this document and summarised below.

4.1 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.

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

4.2 Workflow Messaging

Our Workflow Messaging solution provides access to a fully configurable, omni-channel workflow engine, that sits between your software systems and your stakeholders. It empowers you to create the specific stakeholder engagements that your business needs, without having to customise your software applications and business systems to achieve this. Using workflow messaging allows you to embed automation into everyday processes, boosting productivity and creating a much more streamlined customer experience. You can create fully interactive stakeholder engagements that bring real value to your business, whilst removing both the cost and risk of time-consuming software development.

A full specification for Workflow Messaging is available in Appendix B

4.3 API Messaging

boomAPI

Boomerang's RESTful API delivers an ideal blend of security, functionality, and performance. Offering substantial throughput, it has been designed to meet the needs of enterprise customers requiring instant delivery of omni-channel messaging. The service is fully redundant, supported by a co-located infrastructure and premium connections to Tier 1 carriers, with automated failover inherent to both. It also provides access the next generation of conversational messaging using Boomerang's built-in intelligence guarantees that all messages and responses are matched across concurrent conversation threads. This empowers developers with the ability to build fully automated workflows from your business applications.

A full specification for API Messaging is available in Appendix C

4.4 Microsoft Messaging

Microsoft Custom Connector

Boomerang's custom connector allows organisations to build intelligent messaging solutions from a range of services within Microsoft's Power Platform. The connector exposes Boomerang's omni-channel, Intelligent Messaging solutions to Microsoft Power Automate, Microsoft Power Apps, and Azure Logic Apps. It is the ideal solution for organisations looking to build 1-way or 2-way broadcast messaging, or automated conversational stakeholder engagements, from existing Microsoft applications such as Dynamics 365 CRM, ERP, plus applications with existing connectors such as Azure, IoT Central and Microsoft Teams.

Dynamics 365 Messaging Plug-In

Boomerang's plug-in enables instant access to SMS messaging from any Dynamics 365 application. Where SMS solutions for Dynamics have traditionally been used to broadcast and notify, Boomerang's plug-in overcomes this limitation, automatically matching SMS activities and their associated responses. This enables Dynamics' users to create conversational engagements with stakeholders, as all outbound messages and responses are recorded in a contact's timeline. Crucially, this also creates an opportunity to drive real-time automation into a range of Dynamics' workflow processes, where a response is used as a trigger to initiate further steps in a workflow.

A full specification for Microsoft Messaging is available in Appendix D

4.5 Email-to-SMS and Email-to-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.

A full specification for Email-2-SMS and Email-2-Voice Messaging is available in Appendix E

5 Approach to Information Assurance

The organisation has implemented and operates to a range of information security policies and controls, managed, and maintained via a comprehensive Information Security Management System. We currently hold the following accreditations:

- ISO 27001:2017 certification
- Cyber Essentials and Cyber Essentials Plus certification
- Financial Services Qualification System (FSQS) approved supplier

Additionally, we adopt a best practice approach closely aligned to the following standards and principles:

- Cyber Security – ISO
- Business Continuity Management – ISO 22301
- Quality Management – ISO 9001
- NCSC Cloud Security Principles

The following tools, policies and frameworks have been implemented, including a statement of applicability and objectives for:

- An information security management system (ISMS) covering the organisation and its staff, the products available, and relevant supply chain activity that either processes customer data or has some interaction around it e.g. development of the service.
- Risk assessment and ongoing risk management covering our customer information and related information assets based, around the confidentiality, integrity, and availability of the information. This ensures that appropriate and proportionate policies and controls are put in place, in line with Annex A of the standard, and following ISO 27002 code of practice.
- Regular staff awareness and training, including an HR security lifecycle that covers recruitment, induction, in life management and exit of staff or change of responsibilities
- Governance of the ISMS through performance evaluation at regular intervals, including reviews of policies, management reviews, internal and independent audits as well as processes & tools for corrective action and ongoing improvement.
- Other policies and controls in line with ISO 27002 to address risks and requirements in the areas of:
    - Asset management
    - Access control
    - Cryptography
    - Physical and environmental security
    - Operations security
    - Communications security
    - System acquisition, development, and maintenance
    - Supplier selection and management in life, including a robust segmented approach to supplier work based on the information assets the suppliers have access to in line with the risk assessment
    - Information security incident management (including EU GDPR compliance)

- Information security for business continuity planning and disaster recovery
- Other compliance in line with applicable legislation, privacy, and protection of personally identifiable information

Additionally, our approach to information assurance includes processes and tools for managing specific aspects of EU GDPR such as, privacy by design, Subject Access Requests (SAR) and notifying both the ICO and individuals affected data incidents / breaches. In addition, the organisation has invested in capability for undertaking privacy impact assessments (PIA) and working in line with both EU GDPR and ISO 27001:2017 for information security in projects.

Boomerang's Information Security Policy is reviewed at least annually and is available on the company website.

6 Business Continuity Management and Disaster Recovery Provision

Boomerang is responsible for preparing and maintaining comprehensive business continuity plans (BCP) for its operations and disaster recovery plans (DRP) to ensure that any damage or disruptions to critical assets can be quickly minimised and that these assets can be restored to normal or near-normal operation as quickly as possible.

The plans must be approved annually with the business continuity policy compliance process through the CEO. Testing of the BCP / DRPs at regular intervals, with different aspects of the plans tested, ensuring that all aspects of BCP and DRP are tested at least annually.

Boomerang will also:

- Maintain a strategy for reacting to, and recovering from, adverse situations which is in line with senior management's level of acceptable risk;
- Maintain a programme of activity which ensures the company has the ability to react appropriately to, and recover from, adverse situations in line with the business continuity objective;
- Maintain appropriate response plans underpinned by a clear escalation process;
- Maintain a level of resilience to operational failure in line with the risk faced, the level of negative impact which could result from failure and senior management's level of acceptable risk;
- Maintain employee awareness of the company's expectations of them during an emergency or business continuity threatening situation;
- Take account of changing business needs and ensure that the response plans and business continuity strategy are revised where necessary;
- Remain aligned with best practice in business continuity management;
- Provide a copy of its Business Continuity Plan on request;
- Use recognised standards to provide the guidance and structure for its business continuity activities and all comparable disaster recovery activities.

6.1 Infrastructure

The end-to-end service has been architected so that any single point of failure has been removed, from the data centres and cloud platform to the service applications and messaging suppliers.

Multi-site failover

Multiple data centres support the service infrastructure to provide a zero point-of-failure system. Data spans both geographical sites in real-time, and any data changes to the primary location are also replicated in the secondary location. When failover occurs, both memory and data are captured and replicated, thus removing any transition loss. Data centre services all reside in the UK and are compliant with industry-leading standards.

Cloud solution

The platform has been designed and built to achieve 99.99% service availability. VMware and Kubernetes provide complete hardware and software fault tolerance and multi-site

failover in case of a data outage or network routing issue - full and immediate failover is delivered in real time between the two locations. The cloud architecture and Kubernetes allow the service to auto-scale / de-scale based on consumption, ensuring that surges taking activity beyond expected levels can be easily accommodated.

Network architecture

Network devices dedicated to managing interfacing communications with Internet Service Providers (ISPs) are used. A redundant connection to more than one communication service at each Internet-facing edge of the network is in place, and these connections each have dedicated network devices. Entry points to both networks across all data centres are provisioned with multiple 100Gbit dedicated internet feeds located upstream across multiple network carriers, spanning the whole of the UK. This guarantees the optimum network level integrity and connectivity speeds for both customers and suppliers. The services are built around an assured data transport mechanism and aligned to HMG PSN strategy.

Service applications

The application layer is delivered via a clusterised, scalable cloud based Kubernetes platform with high availability and reliability. Multiple instances of the components used within the delivery of services are in place to avoid a single point of failure. This includes:

- Load balancing internet traffic across multiple instances;
- Use of multiple, independent messaging processing services;
- Multiple messaging queues to ensure substantial volumes of messages can be processed simultaneously;
- Using multiple messaging suppliers across messaging channels and global destinations (for location-specific messaging such as SMS and voice).

As components are modular, this provides the ability to readily upscale processing capacity against each specific component. In the event of an issue at the application level, we can roll back cluster instances in real-time via a SNAP shot that is maintained via our SAN architecture.

6.2 Back-ups

Full daily level 0 backups are taken and held off-site using R1 CDP Data continuity. Backups are held on file for 365 Days and verified after each successful SNAP shot. To complement the daily backup set, hourly checkpoints are also taken and held on a rolling 30-day rotation. The backup set then allows the platform or specific subset of the infrastructure to be rolled forward / backwards at any given time with no data loss. All system files and data are copied to a second storage node for redundancy and availability. Back-ups are regularly tested to ensure that the information and data which has been backed up can be restored in the event of deletion, loss, corruption, damage or made unavailable due to unforeseen circumstances working against our defined backup schedules.

6.3 Monitoring

Comprehensive monitoring with NewRelic and associated external alerting has been implemented across all components underpinning the delivery of Boomerang services.

Network

Both internal and external monitoring are utilised within the data centre facility to monitor all key elements of the network and physical presence. The origin and flow of traffic into our core data centre network switching are inspected for anomalies. The inbound network is also monitored for DDOS attacks against the core switching or BGP issues.

Platform

All key elements of the platform and services are monitored, including but not limited to:

- Availability of service domains / URLs
- Infrastructure - availability and resources utilised (such as disk space, RAM, database queries, connections, queues)
- Supplier platforms
- Trends in live transactional messaging data (e.g. delivery and response success by destination and supplier)
- Service performance (e.g. transit times, throughput, status, and length of message queues

Each component that is monitored will trigger a warning based on pre-defined thresholds being breached and critical status alerts are issued in the event of a failure. These thresholds are reviewed quarterly to ensure their accuracy, relevance, and reliability.

6.4 Capacity Management

Capacity and performance have been considered during the original design and evolution of our services, to ensure they are able to meet expected demand and customer service levels. Our cloud based environment allows for rapid deployment of additional resources where required, without disruption to production services. Cloud instances have also been configured to use an auto-scale set of resource limits, within which additional resources are utilised as demand is increased.

Internal and external monitoring systems are used to track availability and performance. The data captured is used to review the service performance every week also ensuring that customer KPIs are maintained. Metrics are reviewed against customer growth / increased usage, allowing us to project future capacity requirements. These projections also account for new business, in turn allowing us to scale the platform on demand within any area, i.e. CPU / RAM / Disk / Network. Warning thresholds are set at a level that will allow ample time for necessary action to be taken, prior to reaching critical status.

New initiatives relating to the product development must be considered in regard to their impact on performance and resource utilisation. As examples:

- Customer user interfaces are developed to accommodate high volumes of users accessing the application at the same time;
- Transactional processing has been segmented and load balanced so that additional resources can be easily added to the key components in the delivery process;
- Capacity requirements are addressed with relevant upstream suppliers to ensure that end-to-end delivery capacity for transactional messaging can be sustained.

6.5 Change Management

Changes to any system components, configurations, software, and system code are regulated and controlled via a structured change management process to minimise the impact of any changes upon service users. Changes are recorded and evaluated according to their priority, risk, and their impact upon availability of services and changes must be formally approved prior to implementation.

QA Testing

We implement rigorous testing processes to safeguard service availability and minimize the risk of any issues affecting a production release. Testing consists of manual testing and automated using a library of pre-defined and approved test scripts. Changes are migrated through development, testing and pre-production environments, to validate the impact of the changes, prior to their release. Test environments are consistent with the production environment to maintain accuracy across all testing and relevant testing is also undertaken for any changes that could have an impact on security or system performance.

Configuration updates

Updates to operating systems and platform maintenance are carried out quarterly or on an ad-hoc basis for urgent changes. This is to ensure that both cluster and operating systems are secure and up to date. Updates are performed out of hours and are performed with a full rollback policy / SNAP shot in place. Cluster updates and patches at the OS level do not impact the Service or application, as scheduled cluster maintenance can be performed offline without any impact against live services. Any system configuration changes are first deployed in the QA environment for evaluation and risk assessment, and all configuration changes are recorded.

Notification of changes

Customers are notified in advance of any changes according to the terms of the support packages set out below. We endeavour to provide two weeks prior notice where possible and will ensure that a minimum of 5 days' notice is provided.

6.6 Disaster Recovery

In the unlikely scenario that Boomerang is affected by a catastrophic event, processes are in place to restore services with minimal disruption to live services.

- Recovery Time Objective (RTO) – The maximum recovery time before services are fully restored is 30 minutes;
- Recovery Point Objective (RPO) – No longer than one hour.

7 Securing the services

7.1 Network security

Network devices, including firewalls and other boundary devices, monitor and control communications at the network's external boundary and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACLs), and configurations to enforce the flow of information to specific information system services. ACLs, or traffic flow policies, manage the flow of traffic.

A wide variety of automated monitoring systems are used to provide a high level of service performance and availability. These monitoring tools are designed to detect unusual or unauthorised activities and conditions across network usage, port scanning activities, application usage, and unauthorised intrusion attempts. The tools can set custom performance metrics thresholds for unusual activity.

7.2 Cloud security

Services have been designed and implemented in accordance with NCSC cloud Security Principles, which is described in detail Here.

Internal connectivity to the platform is VPN protected, which is secured directly by IP-based and ACL-controlled firewall rules and VPN connectivity. This is also validated by regular scans carried out by an external provider checking the network tier and penetration of different components within the architecture. External access to the core cluster and application platform is permitted by a three-phase approach:

- Inbound connections are verified by the external firewall cluster and that will check to ensure the inbound connection has originated from a trusted IP address.
- Once the initial connection is made, the IP address is then verified by the internal firewall system
- Where access at the IP level is granted, then user-based authentication can take place.

IP access to the production platform is permitted by a strict change control process and revoked once access is no longer needed. User access is defined and SUDO permissions are granted again, based on a strict change control process that is regularly reviewed and approved internally. This level of control also makes it possible to permit access to individual tiers of the platform (the platform is split between web, application, database, and audit logging).

7.3 Application security

All components within the application layer are modular, allowing each component to utilise its own hardware resources while communicating securely with each other. Layering the architecture in this way allows each component to be independently secured using its own firewall. All Service access points (API endpoints and web browsers) are secured using SSL encryption (HTTPS) to protect against data interference. All data is encrypted from leaving the platform until received by the requesting device.

Additionally, all software development processes conform to a Secure Development Policy, which addresses various aspects of the development lifecycle, ensuring that:

- Access to development environments is fully controlled and provide on a need-to-know basis;
- Development environments are secured appropriately, and changes managed correctly;
- Security is considered as part of the design and planning phases;
- Code is developed according to best practice and recognised standards and managed using secure repositories;
- Security forms an integral part of the testing and release strategies.

7.4 Malware prevention

Manual and automated scanners are used to search for websites that may be vehicles for malware or phishing. Multiple anti-virus engines used on servers to help catch malware that may be missed by anti-virus signatures. Support team members are trained to identify and eradicate malware that might infect the network and unusual instances are escalated through to the Operations team. In the event that any Malware is isolated on the production system, this is quickly quarantined, and alerts issued internally. A daily pattern update is performed which ensures that its internal scanning engine is kept up to date.

7.5 Security and vulnerability testing

External tools are used regularly to ensure that security of the service is optimal and that industry standard best practices are continually adhered to:

- Penetration testing – carried out at least annually across our service infrastructure
- Vulnerability Management scans – Carried out against all assets in the Boomerang estate
- Web Application Scans – Checks and verifies that the application code is secure to DDS standards
- Real-time scans running continuously to identify common vulnerabilities

8 Securing data

The overview provided in the earlier section Approach to Information Assurance describes the holistic approach to information and data security that has been embedded across the organisation, in line with our ISO27001 accreditation. This section outlines some key elements that help to secure any data under our control.

8.1 Cryptographic controls

Cryptographic controls are used to secure data across the platform, to protect data at rest and in transit.

Data stored on back up devices

On and off-site backups are stored and encrypted to AES 256Bit Encryption. Access to the backup drives is only possible upon successful verification of the AES Private Key that is protected internally by relevant staff. The AES Encryption mechanism provides a further layer of data safety and protection to all backup data both on and offsite. This key is changed every 12 months to ensure the utmost protection. When a storage device has reached the end of its useful life, procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. These procedures follow NIST 800-88 (“Guidelines for Media Sanitization”) to destroy data as part of the decommissioning process.

Accessing service applications

Access to sensitive data via a web site, web application or mobile application. Encryption is required for accessing sensitive data from anything with a web interface, including mobile devices (i.e. use of HTTPS to encrypt sensitive data). Production web servers (or devices with a web interface) that support secure (HTTPS) connections must have an SSL certificate installed ensuring that the SSL certificate complies with the correct level of 256-bit encryption.

Database

Transport of sensitive data that is part of a database query or web service call (examples SQL query to retrieve or send data from database or a RESTful web service call to retrieve or send data from a cloud application). To protect sensitive data throughout its lifecycle, we use MySQL Enterprise Encryption as standard.

8.2 Access controls

Access controls within Boomerang

Our Access Control Policy, and range of supporting policies, set out a comprehensive range of access controls to safeguard information and customer data. Internal access to company systems and networks holding or processing customer data, is granted on the basis of least privilege. Procedures are in place to ensure that access to systems is formally authorised, and regularly reviewed, to ensure its continued relevance. Every system user is identified by a unique Id and key activities carried out by a user, are logged with the date and time the activity was performed. Asset owners are assigned to, and responsible for, company information assets which includes carrying out regular reviews of system access to make sure that allocated access is up to date (and revoking access that is no longer applicable).

Access controls within services used by customers

User access to services is fully secured with stringent log-in controls, password management and an option to apply 2-Factor Authentication to use access. Logical controls are in place that allow customers to segment user access based on roles and permissions that align to both system functionality. Access to contact data as well as and transactional message data held in the system can be controlled on a 'need to know' basis and messaging data (communication addresses and message content) can be anonymised where required.

Customers using the services are in control of the data imported or submitted to the services. Customers have the ability to modify or delete this data at any time, and all customer data is deleted after a trial or contract period has ended. Boomerang will only access data provided by its customers on request of the customer or where required to investigate a service-related issue.

8.3 Staff recruitment & training

Screening and relevant checks are carried out to verify the suitability of new staff, and both employees and contractors must comply with Boomerang's information security policies as part of their day-to-day duties as part of the contractual obligations. As such, information security training is carried out at regular intervals, with the details recorded within their Personal Development Plan. Any emerging threats, issues, or regulatory requirements that employees should be made aware, communicated to staff in real time, as required. Internal and external audits are also carried out at regular intervals to verify that staff are complying with the policies and controls set out for them.

8.4 Data retention and legislative compliance

Data flows covering personally identifiable information have been mapped across the organisation and retention policies have been implemented to ensure that the controls in place that are proportionate to both the type of data held and the basis by which it was provided. As such, Boomerang is able to maintain compliance with the key principles of data protection legislation (including but not limited EU GDPR 2018).

Alongside the data security controls implemented in accordance with our ISMS, the following policies set out approach to management of personal data.

- Data Protection Policy
- Data Loss Prevention Policy
- Data Management Policy

9 Customer On-Boarding & Off-Boarding

9.1 On-Boarding

Trial service

A trial service is provided, containing full access to service functionality. Trials are provided free of charge, include some free message credit and are active for a period of 14 days (or as otherwise agreed with the customer). Trial accounts are created directly from the Boomerang website, requested via the Boomerang website, or requested by contacting Boomerang directly.

All customer trials are subject to the standard terms and conditions presented when accessing the trial account or agreed to in advance and are also provided via our G-Cloud service offerings.

Proof of concept (POC)

A POC service can be provided. Terms of the POC and the configuration of the service account would be agreed with the customer prior to implementation. Boomerang would make resources available to work with the customer to identify the core objectives and success criteria, providing guidance on how these could be best achieved during the implementation phase and across the duration of the POC.

Production services

The scope of the customer's project will determine the on-boarding approach adopted and the resources that will be allocated to project management. Boomerang will provide assistance to customers migrating from an existing supplier and the following go-live 'gates' must be completed and agreed before services are made live:

- Commercials have been finalised:
  - Purchase order received: A valid purchase order must contain:
    - A purchase order number
    - Details of the services and featured being provided and all associated costs
    - Details to be used on any invoices;
- A signed Call-Off Order Form has been provided;
- The service configuration requirements have been agreed and the account has been provisioned according to these requirements;
- Any training agreed has been completed;
- Customer's user testing has been completed and signed off;
- All customer roles / contact details have been provided (support, operational commercial, finance etc.);
- Support procedures have been provided to the customer;
- A project implementation plan has been agreed by both parties (for larger implementation projects).

Implementation support and training

The services are supported by integration and user guides, detailed help documentation, FAQs, Set-up wizards, videos, and 'Info' buttons (providing users with an understanding of specific functionality in situ). Boomerang also provides user training and implementation support via web-conference or on-site.

Training programmes include ‘Train the Trainer’, ‘User training (general training across a broad base of users)’, or role base training (content focused on specific system / job roles). An inclusive training allowance is provided as part of the service.

A full implementation plan can be provided on request when purchasing the services.

9.2 Customer off-boarding

Termination

Customers must fulfil the minimum contract period agreed, and any service cancellation requests are submitted in writing and will be subject to the agreed cancellation period. The service will remain active up to the agreed cancellation date and upon reaching this date, will be decommissioned so that all subsequent requests to access the service will be blocked. The customer will be obliged to pay any outstanding monies for subscriptions or message transactions that have not already been invoiced. The service account (although not active) will be retained for a further period before being fully deleted from Boomerang’s systems (after which no account data will be retrievable). Any data uploaded by the customer can be modified or deleted as required during the contract period or notice period. The deletion of data involves full hashing over.

Early termination of the contract will incur termination fees if the termination is not result of a material breach.

Any transactional message data processed during use of the services will be held for the standard retention period of 13 months from point of processing, unless otherwise requested by the customer.

Where additional services have been purchased that are still within their contract period (e.g. dedicated or shared inbound short code services), the terms of those agreements remain in place.

Service migration

Boomerang will support customers in the process of migrating to other suppliers. Data can be exported from the systems prior to termination of the service and account access will be available.

Portability of SMS virtual numbers from Boomerang to another supplier is not supported.

10 Service Management

10.1 Background and Overview

The services have been designed to meet the requirements set within legislation and contributes the Government meeting its targets on CSR and Environmental Policy. The SaaS requires no download of software. All services are accessed via a user Interface or an Application Programming Interface (API).

10.2 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

Access to transactional reporting data and analytical data relating to use of the services is provided via the user interface.

10.3 Training services

Training will be provided as part of the on-boarding process. This will be arranged by the customer's Account Manager and conducted by telephone / online, unless otherwise specified. The customer will provide details of all attendees and will provide details of any specific objectives that should be covered in the session. As standard the following items will be covered:

- Account configuration
- Service overview / provisioning
- User interface
- Reporting
- Billing
- Support services

10.4 Service Constraints

Maintenance activities are classified as:

Planned maintenance

Planned maintenance covers scheduled activities that are required to keep the services and infrastructure supporting them secure, error free and optimal. All planned maintenance scheduled where possible to minimise customer inconvenience and the maximum notice period possible is provided (a minimum of one week is mandatory). Notifications containing

details of the maintenance schedule are issued to designated contacts before and on completion of the work.

Unplanned maintenance

Unplanned maintenance is undertaken to prevent service-related issues or degradation of services that would otherwise affect customers' use of the service.

Emergency maintenance

Emergency maintenance is carried out to address any issues affecting availability, provision, or performance of the service.

Although Boomerang will provide as much information as possible during unplanned and emergency maintenance, it may not always be possible to provide prior notice, due to the nature and urgency of the work being carried out.

10.5 Operational service support

Operational support consists of Service and Support requests. Service requests are raised and monitored through our Technical Support case management system. Such requests can be raised directly by the customer or by the Technical Support team.

All service requests are assigned a priority level between one and three, where Priority 1 = Level 1 (High), Priority 2 = Level 2 (Medium) and Priority 3 = Level 3 (Low). Attributing the priority/severity of a request should be based on the definitions provided in our support procedures.

Support requests include 'how to' queries, billing queries and service change requests and should be received from the appropriate customer contact points, as defined in our support procedures.

10.6 Support packages

Two support packages are provided – Standard and Premium. The table below summarises the level of support applicable to each package and Service Level Agreements are only available to customers taking Premium support.

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	24 hours	1 hour
Severity level 2	24 hours	1 hour
Severity level 3	24 hours	1 hour

Service Restoration Target		
Severity level 1	No commitments	3 hour fix time
Severity level 2	No commitments	8 hour fix time
Severity level 3	No commitments	2 day fix time
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 at contracted rate

10.7 SLA penalties and service credits

Premium support customers are entitled to Service Credits based on a failure to meet the monthly System Availability of 99.50%. Where Boomerang fails to meet this target in respect of any calendar month, subject to the paragraph below, Premium support customers will be entitled to claim a Service Credit of 10% of the monthly value of the service subscription paid in respect of the Service affected (being one twelfth of the total annual amount paid). Service Credits are not provided against any other annual or monthly charges (including but not limited to message credits) nor in respect of any other metrics or performance measurements. A Customer is not entitled to Service Credits if it is in breach of its agreement with Boomerang, including without limitation where the Customer is not up to date with its payments when the relevant Outage occurred, or Service Credits are claimed.

10.8 Account Management Service

Account Management Overview and Responsibilities

An Account Manager will oversee service implementation and support the ongoing development of the customer account. Acting as the primary point of contact for discussions around overall service performance the Account Manager will provide regular contact to discuss and analyse key metrics. It is the responsibility of the Account Manager to:

- Schedule and coordinate the account management meetings / reviews
- Proactively deal with issues and concerns escalated by the customer Sponsor.

It is the responsibility of the customer's Sponsor to:

- Participate in the account management meetings / reviews.
- Proactively deal with issues and concerns escalated by the Account Manager.

Pre-Implementation Account Management

Your Account Manager will be available as required, during implementation. The primary focus of the Account Manager during the course of implementation will involve:

- Finalising the contract and obtaining signatures
- Managing the scope of the contract and processing Change Requests / Variation Orders.

- Acting as the point of contact for the customer's Project team, participating in project governance activities as required.
- Establishing the relevant contacts for the customer across the following areas:
    - **Support Contact:** Responsible for overseeing the technical implementation and receives prior notifications concerning any planned or unplanned outages
    - **System Administrator:** Responsible for the day to day administration and account management
    - **Financial Administrator:** Responsible for all financial matters including receipt of invoices, credit notes and account statements.

There are no contractual Service Level Agreements (SLA's) in place for the Account Management service.

Post implementation Account Management

The Account Management model will need to be agreed with the customer, but the standard model is defined below.

- A post implementation courtesy call addressing any questions or issues that may have arisen that week or remain unresolved by the Support Team. Thereafter:
- Quarterly review meetings (by conference call unless a face-2-face meeting is requested)
- Executing post-launch PR activities as agreed with the customer.

Account Management Reporting

The account manager is responsible for reporting:

- Minutes and actions arising out of the monthly review meetings
- The end of contract 'value report' stating benefits derived by the customer from the delivery of the service.

The customer is required to review and sign-off the minutes or otherwise provide recommended changes.

10.9 Ordering and Invoicing

Additional services and features can be purchased directly via the user interface or directly with Boomerang by providing a purchase order.

An invoice covering the annual subscription for the service is issued automatically upon provision of services which requires payment within the agreed payment terms Thereafter, invoices for messaging activity will be provided on a monthly and issued to designated billing contacts on or around the first of each month basis (post-paid customers). As part of the standard billing model:

- All service subscriptions are charged annually in advance
- Messages are billed monthly in arrears or deducted from a pre-paid credit purchase
- All invoices will include a breakdown of message activity and the associated costs by country and accessible from the Billing section of the Boomerang user interface
- Where a pre-paid purchase is made, a receipt is issued by email and is accessible from the Billing section of the Boomerang user interface

- Where a customer specifies any elements of data that are to be automatically deleted on completion of a transaction, these elements will not be included in any reports produced by the service.
- Invoices covering subscription renewals are automated unless Boomerang receives notice to cancel the services according to the terms of the agreement.

Any deviation from this model must be agreed by Boomerang and included in the customer agreement, in the section for non-standard terms and conditions.

All invoicing documentation is provided in PDF format and will contain a summary of all message traffic to have passed through the account, broken down by country along with any fixed subscription charges associated to the account.

Any queries must be directed to billing@boomcomms.com and should also be issued in writing within 20 days of the invoice date. Any unresolved billing queries should then be directed to the Operations Director.

There are no contractual Service Level Agreements (SLA's) in place for the ordering and invoicing service.

11 Customer requirements & technical pre-requisites

11.1 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.

11.2 Technical pre-requisites

User Interface

Boomerang UI is provided as a SaaS solution, as such the user interface must be accessed from a web browser supporting HTTPS 256-bit SSL. Chrome, Firefox, and Safari web browsers are fully supported

End users / message recipients must have access to a device(s) supporting initiation or delivery of messages via the available communications channels.

APIs

TLS - Due to security vulnerabilities with TLS versions 1.0 and 1.1, Boomerang will only traffic using TLS version 1.2 or higher. For enhanced performance and security, we recommend that customers connect using TLS version 1.3.

HTTP - For optimised performance we also support connections with HTTP/2.

Appendix A – Functional specification for Broadcast Messaging

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.

Communication Channels

International messaging is supported via:

- SMS
- Voice (delivered as Text-to-Speech)
- Email
- WhatsApp
- RCS (Rich content messaging)

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)

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

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

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)

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

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)).

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 B – Functional specification for Workflow Messaging

Communication Channels

International messaging is supported via:

- SMS
- Voice (delivered as Text-to-Speech)
- Email
- WhatsApp
- RCS (Rich content messaging)

Messaging Solutions

The following messaging solutions are supported:

- 1-Way Messaging via all channels
- 2-Way messaging via all channels
- Intelligent 2-Way messaging via SMS, Email (recipient replies are matched to each individual broadcast)
- Conversational messaging via all channels (conversation threads are created and managed according to subject matter
- Inbound messaging (receiving end user / system initiated messages)

Example Uses

Template workflow solutions are used to fulfil and end-to-end communications process. Examples of available solutions / uses are listed below.

- Lone worker - Duty of Care
- Incident communications
- Field Force communications
- Customer Satisfaction Surveys (SMS / Web)
- Contact Centre Engagement
- Service Desk Ticketing
- Business Continuity communications
- Machine-2-Machine alerting
- Service Outages (SLA compliance)
- Appointment Rescheduling
- Resource Management - Workforce Fulfilment
- Shift Planning
- Automated Marketing Campaigns
- Information Requests / Booking requests
- Debt Recovery
- Logistics - Delivery Management
- Mustering - Personnel Recall
- Instant authentication (2FA)

Workflow Engine

The workflow engine fully configurable, allowing any type of communication workflow to be configured to meet a wide range of bespoke requirements. Workflows within the same project can actively interact, sending and receiving to and from each other, enabling fluid and dynamic workflow configurations.

A summary of some key features are listed below:

- Drag-and-drop interface for easy workflow creation
- Multichannel orchestration for seamless cross-channel experiences
- Multi-step workflows with conditional triggers
- Dynamic content personalization based on external data sources
- Conditional logic and branching for dynamic workflow paths
- Template library for pre-designed workflow templates
- Customisable workflow templates for different industries or use cases
- Collaboration tools for team-based workflow design
- Standard integrations with 3rd party applications and software
- Workflow simulation and testing environment
- Role-based access control for workflow editing and deployment notifications
- White labelling for brand consistency
- Custom API endpoints for third-party integrations

Workflow Components

Workflows consist of various components that perform different functions within the communication process.

Activation channels

Workflow Projects can be activated on demand via the following channels:

- HTTPS
- Email
- SMS
- User Interface
- Third party software integration

Activation functions

Functions available when configuring the activation criteria or when activating a workflow project are listed below:

Data Extraction

Create variables to define the data that will be extracted from the activation request submitted by the remote application or service and used in the workflow. If the workflow is activated from the user interface these variables are presented in the web form used to activate the process.

- Extract Recipients from an activation request – Create the variable(s) against which recipient data will be passed (mobile number, email address etc)
    - Dynamic grouping – Categorise and group recipients according to variables passed in the activation requests (e.g. List 1- Primary On-Call Team, List 2 – Stand By Team, List 3 - Supervisors). These groups can then be used in workflows as required

- Extract Data from the activation requests – Create the variables against which other data included in the activation request will be extracted. These variables can be used to:
    - Set the activation criteria – The value or combination of values passed against the variable will be used to activate the workflow
    - Create tokens - Tokens are inserted into message content and the values passed against the selected variables will replace those tokens when delivered to the recipient
    - Categorise data variables – Amalgamate variables into categories (e.g. categorise List 1, List 2 and List 3 could be categorised as 'Recipients' and used in a workflow which issues communications to all recipient)

Activation Criteria

Define the rules and actions that are applied when a request to activate a workflow project is received:

Start workflow

Start a Broadcast / Workflow:

- Immediately on receipt of request
- Schedule Activation:
    - Activate at set time
    - Schedule based on a time variable included in the activation request
    - Schedule for a specified period before / after variable date and time
    - Localise date / time data according to recipient time zones

- Create activation conditions:
    - Activate based on content contained in the inbound request (e.g. a variable value or combination of variable values, keywords, or text string)
    - Activate when a specified count of inbound requests is reached
    - Activate when a specified count of inbound requests is reached containing specified content
    - Activate when a specified count of inbound requests reached from a specified sender address (or combination of addresses)
    - Activate when an inbound request not received within a specified time period
    - Activate if a specified count of inbound requests not reached:
        - Within a specified period of time or by specified date / time
        - That contain specified content within a specified period of time) / by specified date / time
- Validate activation requests
        - Validate the inbound sender address
        - Validate IP address / Server address

        - Request 3rd party approval before activation
        - Manage duplicate requests
        - Validate the content of inbound requests
            - Validate recipient data (e.g. format of telephone numbers, email addresses etc)
            - Normalise telephone numbers to recognised standards
            - Validate date and time data (e.g. check if date / time is in the past)

Manage inbound senders

- Group / categorise inbound sender address using combinations of:
    - All sender addresses submitting a request to a specified inbound address
    - Sender addresses with specified content contained in the inbound request
    - The communication channel via which the request was submitted
- Remove inbound sender address from an existing group / category using combinations of:
    - All sender addresses submitting a request to a specified inbound address
    - Sender addresses with specified content contained in the inbound request
    - The communication channel via which the request was submitted

Broadcast Features

The Workflow Engine offers a range of broadcast features incorporating a wide range of communication channels.

Omni-Channel Messaging

Create 1-Way or 2-Way broadcasts across the following channels:

- SMS
- Email
- Voice messages (text-to-speech)
- Voice calls (connect recipient to a telephone number)
- WhatsApp
- RCS

Broadcast attributes

When creating a broadcast users define the following:

- Communication channel(s) used (selecting from the available communication channels)
- Content of the broadcast message (same per channel / customised per channel)
    - Options to format content according to the channel used (e.g. HTML email or images / branding in RCS and WhatsApp messages)
    - Options to include dynamic variable data:
        - extracted from an activation request
        - received from another workflow
        - based on workflow events / behaviour
- Recipients of the broadcast
    - Stored contacts / distribution lists (containing multiple contacts)
    - Dynamic contacts – Contacts are identified according to:
        - Attributes associated to the contact

        - Categorisation – association to a pre-defined category (e.g. ‘Opt-in Requests’)
        - Workflow behaviour (e.g. responding to message, responding with a specified content, responding after a specified period of time, failing to respond etc)
        - Association to a scheduled calendar event
    - API Contacts
        - Contacts are included / passed in the request to activate a workflow project
        - Contacts are retrieved via a request to a third-party application when the broadcast is initiated

Broadcast Logic

Implement rules to determine how and when broadcasts are processed.

- Single channel broadcast
    - Same message content sent to all recipients
    - Custom content sent to different recipients / distribution lists
- Multi-channel broadcast – all communications channels are sent simultaneously
    - Same message content sent to all recipients
    - Content customised per communication channel to all recipients

As broadcasts can be initiated concurrently, it is possible to use any combinations of the above, to allow bespoke content to be sent according to different recipients / distribution lists, and / or different communication channels.

- Staged / staggered broadcast – communications are scheduled at pre-defined intervals, with options to send:
    - Same content sent via the same communication channel (e.g. pre-scheduled reminders)
    - Same content via different communication channels
    - Custom content per communication channel
- Broadcast Direction - When creating a broadcast set the direction, choosing between:
    - 1-Way – No reply handler configured
    - 2-Way – Reply handler configured allowing rules to be configured relating to the management of responses
- Broadcast features
    - Social hours – Messages are only processed between specified times (unless flagged as priority)
    - Data overwrite – Sensitive content is overwritten
    - Number masking – Set up conversations between external parties (e.g. an engineer and customer) without disclosing personal numbers
    - Short links – Long URLs are converted to short links
    - Web Forms – Configurable web forms are embedded in a message via a short link

- Document management – embed links to stored files to record digital signatures, acceptance of terms and conditions, and acknowledgements denoting that a document has been viewed / read
- Geolocation mapping – Trigger broadcasts based on the location of a mobile devices

Delivery statuses

Message delivery statuses are returned from the recipient's communication service provider denoting that a:

- Message has been delivered to recipient's device
- Content has been delivered (i.e. messages has been read / listened to)
- Message has failed to deliver
- A message has been submitted to the recipient, but delivery is pending

Rules and actions can be implemented according to different status categories:

- Positive Delivery Status / Read status
  - Notify on status returned (e.g. a third-party)
  - Categorise / group recipients by delivered status
  - Update contact record with latest status
  - Count positive statuses returned
  - Notify when specified quantity of positive statuses returned
  - Trigger reports on positive delivery statuses across a range of criteria

- Negative delivery / read status (failed to deliver)
  - Send a repeat message
  - Escalate communications to recipient via a different communication channel
  - Escalate communications to a different recipient
  - Escalate on count of failed statuses returned
  - Notify on status returned (e.g. a third-party)
  - Notify when specified quantity of negative statuses returned
  - Categorise / group recipients by failed status
  - Update contact record with latest status
  - Trigger reports on negative delivery statuses across a range of criteria

- Pending delivery (no positive or negative status returned)
  - Send a repeat message
  - Escalate communications to recipient via a different communication channel
  - Escalate communications to a different recipient
  - Categorise / group recipients by pending status
  - Trigger reports on pending delivery statuses across a range of criteria

Reply Handler

Where the reply handler is enabled for 2-way communications across all channels, conditions and actions can be implemented according to reply behaviour, where for example:

- Any reply is received

- Any replies containing specified content / keywords received (any number of variations can be implemented)
- A specified count of replies is reached / not reached
- A specified count of replies containing specified content is reached / not reached
- Replies are received within / outside of a specified time period
- A reply that does not match specified content is received
- Duplicate replies are received from the same responder
- A reply is / is not received from a responder in a specified category or group
- A reply is received during / outside of a specified workflow status (current workflow or any other project workflow)

These conditions or combination of conditions provide the ability to trigger further workflows incorporating the actions below:

- Create a subject based conversation thread with the responder (single or concurrent)
- Repeat a message
- Escalate communications to a different channel
- Escalate communications to a different recipient or distribution group (via the same or alternative communication channels)
- Trigger a broadcast to a separate distribution group
- Group / categorise responders
    - by response content / keywords
    - time of response (inside / outside of specified milestones)
    - if response received within / outside of specified count quota
- Remove responders from a group / category based on
    - by response content / keywords
    - time of response (inside / outside of specified milestones)
    - if response received within / outside of specified count quota
- Add or remove non-responders to / from a category or group
- Update a stored contact record with reply status or content
- Trigger reports on reply statuses across a range of criteria

Timed Events

Timed events allow configuration and execution of a range of workflow actions based on time based milestones.

- Fixed Time Events
    - Trigger an event at specified date / time
    - Schedule a recurring event at specified dates / times
    - Schedule events based on time / date variables

- Offset Events (before / after)
    - Trigger an event based on real time offset
    - Trigger scheduled and recurring events based on an offset period against the scheduled time
    - Trigger events based on offset time variable

- Runtime / Duration

- Trigger an event when a time based milestone is reached (e.g. intervals between broadcast messages)
- Apply wait times for:
    - Responses to 2-way broadcasts
    - Specified response quotas
    - Delivery statuses associated to specified recipients / groups
    - Specified quotas of delivery statuses
    - Specified quotas of delivery statuses associated to specified recipients / groups
- Define workflow runtime based on:
    - Setting the total duration as a period of time (e.g. 24 hours)
    - Applying a specific end date / time (e.g. complete at dd/mm/yy hh:mm)
    - A variable value / variable offset value
    - The aggregated duration of other workflow events
    - Other workflow events (e.g. stopping a workflow when specified conditions are met)

- Calendar / Scheduler
    - Activate workflows based on pre-defined calendar events
    - Determine recipients based on groups associated to a calendar event (recipients are selected dynamically from the calendar event based on the time a broadcast is triggered)
    - Dynamically filter groups based on date and time fields
    - API request to external calendars in third party software

Appendix C – Functional Specification for API Messaging boomAPI

The API specification is set out in SwaggerHub and accessed via

https://app.swaggerhub.com/apis/BoomerangMessaging/boomerang-messaging_direct_api/1.6#/

Appendix D – Functional Specification for Microsoft Messaging

Microsoft Custom Connector

The functional specification for Boomerang's Custom Connector can be accessed via https://learn.microsoft.com/en-us/connectors/boomappconnect/

Dynamics 365 Messaging Plug-In

The functional specification for Boomerang's Dynamics 365 Plug-In can be accessed via

https://boomlink.uk/d/s/tF6qRWvXDVtKOmrRUK6xHSA3rwWp6K7S/rX0iqLRq2smeu0_P0r2yMBsiFfYBj5UZ-bb3qzxi7Tws

Appendix E – Functional specification for Email-to-SMS and Email-to-Voice Messaging

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.

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.

Communication Channels

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

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

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.

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

Reporting

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.

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