boomCast Service Definition
G-Cloud 13

Contents

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. The diverse range of products, accessed through the intuitive User Interface can be tailored to be used to complement each other or individually. As a communication specialist,Boomerang I-Comms focusses on delivering high quality 1-way, 2-way and intelligent 2-way messaging solutions across different messaging channels. The underpinning Boomerang threaded Technology is patented in over 50 countries around the World the technology used in our services and products is unique. It addresses many of the problems inherent in business communication today.

2 Overview of boomCast for G-Cloud

oomCast is a versatile messaging application used to manage messaging campaigns. It provides access to a range of messaging solutions that help to drive business communications from a single location. Intelligent Messaging joins an organisation's business systems to its distributed stakeholders, so that everyday processes can be automated without the need for specialist equipment or user training.
This signifies a departure from conventional 2-way messaging solutions because it matches all outbound messages and replies, regardless of the quantity sent or the order by which replies to those messages are returned.
This means that a message transaction is no longer limited to simply notifying and informing but can now provide stakeholders with a set of options. The stakeholder's response to one of those options can then be used as the trigger to move a process to its next phase.

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

- 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)

As the service is provided a SaaS solution, the only requirement for access is a web browser supporting HTTPS TLS 256-Bit encryption.

3 Approach to Information Assurance

The organisation currently complies with a range of requirements, policies and controls, including Cyber Essentials, NCSC Cloud Security Principles and operates to security level IL3 . It also achieved ISO 27001:2017 accreditation, the international standard for information security. 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 over G-Cloud, 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.

4 Business Continuity Management and Disaster Recovery Provision

4.1 Policy

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.

4.2 Infrastructure

The end-to-end service has been architected in such a way that any single point of failure has been removed – ranging 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 as data spans both geographical sites in real time, and any data changes to the primary location, are also replicated to the secondary location. When failover occurs, both memory and data is captured and replicated, thus removing any transition loss. Data centre services all reside in the UK and are compliant with the industry leading standards.

Cloud solution

The platform has been designed and built to achieve 99.99% service availability. VMware provides full hardware fault tolerance along with multi-site failover in the event of a data outage or network routing issue - full and immediate failover is delivered in real time between the two locations. The cloud architecture allows 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 that are 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 a 1G bit dedicated internet feed, 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 scalable cloud based platform with high availability and reliability. Multiple instances of the components used within 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 are able to roll back cluster instances in real time via SNAP shot that are maintained via our SAN architecture.

4.3 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 compliment 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 / backward 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.

4.4 Monitoring

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

Network

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

4.5 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.

4.6 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 set 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 full roll back 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 off-line 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 endeavor to provide two weeks prior notice where possible and will ensure that a minimum of 5 days' notice is provided.

4.7 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.

5 Securing the services

5.1 Network security

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

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

5.2 Cloud security

Internal connectivity to the platform is IPSEC secured directly by IP based firewall rules. 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).

5.3 Application security

All components within the application layer are modular, allowing each component to utilize its own hardware resources, whilst 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.

5.4 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.

5.5 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:

- 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

6 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.

6.1 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.

6.2 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.

6.3 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 employment record. 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.

6.4 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).

7 Customer On-Boarding

7.1 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. 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 when accessing the trial account and are also provided in G-Cloud.

7.2 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.

7.3 Production services

The scope of the customer's project will determine the on-boarding approach adopted by and the resources that will be allocated to project management. However, the following go-live 'gates' must be completed and agreed:

- 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).

7.4 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 towards 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.

8 Customer off-boarding

8.1 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.

8.2 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.

9 Service Management

9.1 Background and Overview

The service has been designed to meet the requirements set within legislation and contributes the the Government meeting its targets on CSR and Environmental Policy.

9.2 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 settings
- Addition of services, products or features
- Amendment of existing service, product or feature selections
- Access to transactional messaging data

Reporting
Access to reporting data is provided via the user interface or on request to Boomerang.

9.3 Training services

Training will be arranged by the customer's Account Manager and conducted by telephone / webinar, 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

9.4 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.

9.5 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.

9.6 Support packages

Two Boomcare 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	Boomcare Standard Support	Boomcare 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	99.99%

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	12 hour fix time
Severity level 3	No commitments	2 day fix time
Scheduled Maintenance		
Notice period	5 days	5 days
Actions per month	No commitments	Maximum of 2
Terms		
Minimum term	N/A	12 months
Payment terms	N/A	12 months in advance

*Chargeable at contracted rate

9.7 SLA penalties and service credits

Boomcare Premium customers are entitled to Service Credits based on a failure to meet the monthly System Availability of 99.99%. Where Boomerang fails to meet this target in respect of any calendar month, subject to the paragraph below, Boomcare Premium 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.

9.8 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.

9.9 Ordering and Invoicing

The customer will provide a purchase order (including a valid purchase order number) which will specify the Boomerang products, services and features required along with their associated costs and the required quantities of each. Any additional service features that are required after the initial account configuration must be purchased using a separate purchase order.

An invoice covering the annual subscription for the service is issued automatically upon account creation which requires payment within 30 days of issue. Thereafter, invoices 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
- All invoices will include a breakdown of message activity and the associated costs by country
- 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 received notice to cancel the services according 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.

10 Customer requirements & technical pre-requisites

10.1 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.

10.2 Technical pre-requisites

[BOOMERANG UI]

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 SMS, Email and voice calls (and data in order to receive messages to the Boomerang messaging app)

BOOMMAIL

Access to an email client with the ability to send and receive emails and the email addresses for all users that required access to the service must be provisioned. For additional security, a mail server address or IP address from which the emails will originate is required.

11 Environmental Compliance

The cloud based SaaS fits easily into a carbon reduction policy and has little to no impact on the environment. The office environment is ‘paperless’ by default and contributes to the Government’s drive to reduce carbon emissions.

12 Service Pricing

Services are available from £0.027 per message.

There are not on-boarding charges.

Full Service Pricing is available on the Digital Marketplace website.

- Boomerang I-Comms offers a range of products to complement Boomcast with include: Boomerang API Builder: - Threaded “Intelligent” messaging via API
- Boomerang plug-in: - Microsoft Dynamics CRM for Boomerang
  Boomengage: - Engagement and customer services interactions
- Boomcast Incident Hub: - Management of communications during an incident
- Boommail: - “Intelligent” messaging over email
- Boomlocal: - International 2-Way messaging using local numbers
- Boomflow: - Automatically manage the availability of resources
- API Builder: - API tool that allows the easy connection to 3rd party Apps

To find out more, our products are listed on the Digital Marketplace or contact (Public Sector Account Manager) for a Free Consultation on how our products can benefit your Department.