



BroadSoft Information Security

White Paper



Introduction

Security confidentiality, integrity, availability and compliance are core components of BroadSoft's cloud services offerings. Security safeguards implemented for the BroadCloud services meet the policy and control requirements as set forth in BroadSoft's System Security Framework.

BroadCloud has adopted ISO 27001:2013 and NIST 800-53 as its security framework deployed in the US, European Union and Australia.

At this current time,

- » BroadWorks - ISO 27001:2013 SOA - Available 2017 Certification
- » BroadCloud - ISO 27001:2013 SOA - Available 2017 Certification

Security Overview

BroadSoft's ISO 27001:2013 Statement of Applicability (SOA) certification broadly encompasses 14 control categories.

The areas of audit, controls and certification include:

1. Security Policy
2. Compliance
3. Organization of Information Security
4. Human Resource Security
5. Asset Management
6. Access Control
7. Cryptography
8. Physical and Environmental Security
9. Operations Security
10. Communication Systems
11. Information Systems Acquisition
Development and Maintenance
12. Supplier Relationships
13. Information Security Incident Management
14. Business Continuity Management

Security Policy

Information, information systems, and all related assets are critical and vitally important to BroadSoft, BroadCloud business processes. BroadCloud protects information assets in a manner commensurate with their sensitivity, value, and criticality. Security measures are employed regardless of the media on which information is stored, the systems that process information or the methods used to transport information.

BroadSoft manages its information security policy using a Security Life-Cycle Management process. This process includes the following components focusing on Policy:

- » Security Life-Cycle Review
- » Ratification, Approval and Implementation
- » Annual Review, Updates (as necessary), and Recertification.
- » Annual Communication and Awareness Training
- » Exceptions Management

Compliance

The service and systems are in queue for ISO audit and certification. ISO is annually reviewed for recertification.

Organization of Information Security

The Management Team is responsible for oversight and governance to the Policy Life Cycle process ensuring that services security posture, policies and practices are implemented, updated and communicated to staff and other parties as appropriate. The Operations and Engineering Teams are responsible to deploy IT systems, services, and processes consistent with these policies. Security controls and practices for protection includes restricting access to information and information systems based on the principles of "least privilege" and "need-to-know." BroadSoft's functional business management ensures that all assets, including information and information systems, have appropriate operational and technical measures in place to ensure that customer data and service availability are protected based on risk. To achieve this objective, management conducts annual reviews of the risks to its collective. Similarly, whenever a major security incident indicates that the lifecycle protection of these assets is insufficient, management takes prompt remedial action to reduce exposure and thus mitigate the risk of harm to an asset. Information security training, guidance, direction, and authority are centralized within BroadSoft's Corporate Security Team, which is responsible for establishing, maintaining and monitoring the enterprise Information Security Management System (ISMS), comprised of policies, standards, guidelines, and procedures.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

The BroadSoft Corporate Security team will communicate recommended policy changes to management and relevant members and parties as business needs dictate, or at least annually. BroadSoft security performance is evaluated on an annual basis by an external 3rd party security firm specializing in domain specific security standards. BroadSoft security policies are reviewed and revised at least once annually or on an as-need basis.

Human Resources

Background Check

BroadSoft has established a Background Check Policy to set forth the process and procedures related to the conduct of FCPA and other background checks for designated individuals and entities.

Terms and Condition of Employment - Acceptable Use Case

Employees and external party users using, or having access to BroadSoft assets, are made aware of the policies concerning their acceptable use as defined in the BroadSoft Policy and IT Handbook. All employees and contractors are required to sign-off on having read and understood the BroadSoft Policy and IT Handbook. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.



Training

All employees undergo extensive security training as part of the orientation process and receive ongoing security training annually. Depending on their job role, additional training on specific aspects of security may be required.

Information Classification, Asset Management

Information Classification

Information classification assures that assets are applied an appropriate level of security and protection based on content sensitivity and value of asset to business service and business continuity.

Management and resources maintains strict control over the internal or external distribution of any kind of media, including the following:

- » Classify media so the sensitivity of the data can be determined
- » Destroy media when it is no longer needed for business or legal reasons

Shred, incinerate, or pulp hard-copy materials so that the cardholder data cannot be reconstructed. Secure storage containers used for materials that are used to be destroyed.

Asset Management

Infrastructure asset management is the combination of management, financial, economic, engineering, and other practices applied to physical assets with the objective of providing the required level of service in the most cost-effective manner.

BroadCloud implements an Infrastructure Asset Management inventory of systems and components, which consist of a method to accurately and readily determine owner, contact information and purpose of asset. Asset Management shall include inventory of physical hosts as well as VMs.

Operations Management is responsible for all assets deployed within the service platform environment. Unmanaged or not serviceable assets within the environment are not permitted. If an asset is discovered within the environment that is not managed, it must be either assimilated under the Operations management responsibility or removed and or blocked from the environment.

Maintain inventory logs of all media and conduct media inventories at least annually, and at time of asset moves, adds, changes and disposal.

Access and Control Security

The service ensures that the appropriate levels of access controls are defined and implemented in the operating environment. Access controls consistent with this policy is applied to each system, application, database, or network utilized to manage various types of data classifications and the users that access that data. These controls consist of standardized processes for requesting, approving, granting/revoking, modifying user access, user role definition, and segregation of duties analysis, least privileged access, user password, user identification policies and standards, user access auditing expectations; and network access control list and auditing of network and access activities.

Access Control Policy requires the implementation of user accounts and access controls for systems and applications requiring access to configuration and information. The scope of the policies and controls are limited to access to the Infrastructure and applications owned and operated/managed by BroadSoft Services. User account and access controls shall meet minimum security requirements as specified herein.

- » All users are assigned unique IDs and must authenticate for access to assigned privileged components
- » IDs and authentication credentials shall not be distributed beyond the single user and or group/shared credentials are not shared/distributed
- » Control addition, deletion and modification of user IDs, credentials, and other identifier objects
- » Restriction of access to privileged user ID to least privileges necessary to perform job responsibilities

- » Privileged users shall be identified for specific access
- » Immediately revoke access for any terminated users
- » Remove / disable inactive user accounts
- » Manage IDs used by third parties to access, support or maintain system components

These controls are defined, approved, implemented and overseen by management or designated security officers. These controls are reviewed for accuracy and effectiveness at least annually both internally and by an independent auditing authority.

Cryptography

Cryptography is required as a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography concerns itself with the following four objectives:

1. Confidentiality (the information cannot be understood by anyone for whom it was unintended)
2. Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)
3. Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)
4. Authentication (the sender and receiver can confirm each other's identity and the origin/destination of the information)

BroadCloud documents and implements procedures to protect keys used to secure stored cardholder data against disclosure and misuse.

Physical and Environmental Security

Data center and cloud partners are evaluated annually for SOC2 attestation of compliance in the areas of physical security perimeter, physical entry controls, securing offices, rooms, and facilities, protecting against external and environmental threats, working in secure areas, supporting utilities, cabling security, and delivery and loading zone.

Operations Security

Platform Security

Network services engineers harden and patch the operating systems and infrastructure to protect its systems from various security vulnerabilities. Servers must deliver data in a secure, reliable fashion. Operating system, middleware and application hardening involves:

- » Security sensitive hardened installations
- » Protection of malware
- » Implementations and configurations of robust logging
- » Strong authentication
- » Encryption of sensitive communications
- » Prudent configuration of access controls, "least privilege" and "need-to-know"
- » Information Backup

Hardened platforms with appropriate access and controls further restrict system capabilities to only those that are explicitly required and tolerated for expected system functionality. Systems and software versions and upgrades are cross-checked and undergo suitable testing in a staging environment prior to acceptance for production deployment and use. Technical vulnerabilities of information systems are monitored and logged. The Operations team evaluates any exposures to such vulnerabilities and takes appropriate patch management life-cycle measures to address any associated

risk. Procedures monitor the use of information processing facilities, and the team regularly reviews these activities.

Segregation of Duties

Segregation of duties is enforced as a method for reducing the risk of accidental or deliberate system misuse. Due diligence with policies, process and procedures prevents any single person from accessing, modifying or using assets without authorization or detection.

The initiation of an event is separate from its authorization. The design of these controls provides for oversight and governance to the possibility of collusion.

Development, test and production environments for IT Infrastructure and Applications are segregated to reduce the risk of unauthorized access or changes to operational systems. The team establishes, documents, and reviews an access control procedure based on business and security requirements for access. Configuration and application code is stored in an encrypted, secure database.

Logging and Monitoring

The operations team has extensive operational processes to support high availability. These processes include the selection of key human resources, support and contact processes, system logging, monitoring, system testing processes, and network performance. Any anomaly result in alarms and are address based on severity

Operations continuously monitors all servers, internet connectivity, latency, availability, bandwidth, and severity in maintaining these server network performances. All operational and security logs are retained for extended periods of time to ensure extended availability. The network operations team regularly reviews these logs as part of capacity planning.



Network Communications Security

Information and systems interconnected by the networks are important business assets. Maintaining, and ensuring network security at all levels is essential. Operations achieves this network security through both technical means and management procedures. Network security includes the following:

- » Demilitarized Zone
- » Firewalls
- » Intrusion Detection
- » System Authentication
- » Data Encryption

The security management team determines the security features, service levels, and management requirements of all network services. The team manages and controls the networks, not only to protect them from

threats, but also to maintain security for the systems and applications using the network, including information in transit. Detection, prevention, and recovery controls, along with appropriate user awareness procedures, protect against malicious code. Audit logs record all user activities, exceptions, and information security events. The operations and security team preserves these logs to assist in future investigations and access control monitoring. Independent reviews are conducted on a regular basis to ensure that information security processes are adequate, complete, fit-for-purpose and enforced.

Software Development Life Cycle

BroadSoft has adopted a corporate level Security Software Development Lifecycle (SSDL) to ensure that all applications have consistent security postures and embrace security by design principles. All applications undergo security testing and scan validations for OWASP secure coding practices as part of the development lifecycle.

Vendor Management – Supplier Relationships

BroadSoft manages a vendor security assessment program to ensure that all 3rd party services provided to BroadCloud maintain a security posture commensurate with security risk and compliance requirements. As part of the program, key vendors are periodically reevaluated to ensure that there are no changes to their security posture.

Change Management

Change Management is an important facet of service management, and a standard process by which change is introduced into the service delivery network is crucial to successful implementation of the change. Change is initiated by a variety of groups: engineering, systems engineering, service management, support, professional services and even customer. It is important that the process of implementing any change is designed, reviewed, communicated across all organizations and performed within a well-advertised time window. This allows all stakeholders to be informed about the change,

anticipate issues from any perspective, be aware of it occurring and be able to attribute anomalous behaviors, should they occur to the change being introduced. Broadsoft maintains a public web page <https://status.broadsoft.com/> that provides real time information on BroadCloud scheduled maintenance.

Customer Support

Customer Support engineers ensure that all systems and client applications are up and operational by utilizing tools that continuously monitor the health of every system component. These tools alert personnel at the first sign of any problem so that potential issues can be resolved even before they impact the operations of the network. These tools can also initiate automated problem resolution procedures (such as running diagnostics). Support engineers also monitor network operation and respond to network emergencies but also provide a critical communication link between customer support and its clients. Support engineers record customer-reported problems in an automated problem-tracking system, and coordinate the on-going work necessary to quickly resolve them to the client's satisfaction. BroadSoft maintains a public web page <https://status.broadsoft.com/> that provides real time information on BroadCloud operational status.

This policy, together with the tiered support structure, ensures that a support incident will never reveal private data to an unauthorized person.

Information Security Incident Management

BroadSoft's Incident Response Plan Management Manual follows the National Institute of Standards and Technology (NIST) 800-61 Computer Security Handling Guide. Incident Management policies identified in and applied to services who are providing a business-critical service, or maintaining any application, software, or hardware which supports a business-critical service. The goal of Incident Management is to restore normal service operations as quickly as possible and minimize the impact on business operations. Normal service operation is defined as operating within the agreed Service Level Agreement (SLA) limits. BroadSoft documents policy and procedures to handle security incident response and evaluation. Security Incidents shall be responded to in seven stages: identify, document, communicate, contain, assess, recover and eradicate.

Business Continuity and Disaster Recovery

The BroadCloud is stable, secure, and highly available. All platform components are deployed in a redundant architecture with no single point of failure. These hardened data center sites feature fully redundant fiber optic network access, power grid access, power generation and air handling, and are protected by a dry fire suppression system and state-of-the-art physical and electronic security systems. The data centers are located in various geographic regions within the US. All data



centers operate in active/ active mode with real-time application replication across the regions. Sites share normal call handling load. In the unlikely scenario of a data center disaster, the remaining datacenters are still capable of handling 100% of planned daily traffic. Business Continuity Plan mandates a complete switchover of traffic between data centers within minutes. Every single data center installation must provide a full peak capacity based on historical and predicted future traffic to accommodate unforeseen caller traffic. Business Continuity and Redundancy processes are tested regularly as part of site maintenance requirements.

Summary

Protecting sensitive customer information and keeping up with the increasing number of security standards is expensive and can become overwhelming for any organization. BroadCloud provides for comprehensive levels of security inclusive of the overall hosting package.

ABOUT BROADSOFT

Cloud Business Communications, Team Collaboration, and Contact Center SaaS

	Company	NASDAQ: BSFT	\$341M Revenue (2016)	22% CAGR Since '10	1,750 Employees (Q4 2017)	80+ Country Presence
	Channels	25 of the top 30 service providers by revenue		600+ Channel Partners	\$19B Business lines installed base (Q4 2017)	

Corporate Headquarters | 9737 Washingtonian Blvd | Suite 350 | Gaithersburg, MD 20878

Contact | P: 301-977-9440

General Inquiries | bsb-info@info@broadsoft.com

Press and Analyst Relations | pr@broadsoft.com

www.BroadSoft.com | [Twitter](#) | [LinkedIn](#)