Infobip

Technical and Organizational Measures

Table of Contents

Introduction

Infobip is a global cloud communications platform (Platform) that enables businesses to build connected customer experiences across all stages of the customer journey at scale, with easy and contextualized interactions over customer's preferred channels. Accessed through a single Platform, Infobip's omnichannel engagement, identity, user authentication, security, and contact center solutions help Customers and partners overcome the complexity of consumer communications, grow their business, and increase loyalty– all in a fast, secure, and reliable way.

The platform processes immense volumes of traffic while supporting hundreds of features that customers need and demand. The platform has been designed from the ground up keeping in mind the flexibility of features which can be developed and the speed at which the Platform can be adjusted to accommodate the ever-changing customer's needs. Infobip' Platform provides connecting users through the Internet and extending their reach into the telecom networks, serving thousands of customers around the world, reaching the majority of the world's population.

The platform is entirely developed and maintained by Infobip. Information security and the protection of privacy are of utmost importance and related technical and organizational measures are deeply embedded in every aspect of Infobip and the Platform.

Information security policies and organization of information security

Information security in Infobip is organized using the Information Security Management System (ISMS) framework. Management Board provides strategic objectives and resources for the establishment of ISMS, the execution and operational management of ISMS objectives are achieved by Chief Information Security Officer (CISO) and Corporate Security Department. Management of control objectives related to privacy and protection of personally identifiable information (PII) is managed by Chief Privacy Officer (CPO) and executed by Corporate Privacy Department.

Policies define objectives and procedures define methods on how to achieve specific objectives within information security and privacy domains. Policies and procedures are formally approved, published, and communicated to all Infobip employees and third parties. All policies and procedures are subject to periodic or ad hoc reviews and updates to preserve alignment with a dynamic environment. Policies and procedures define accountability and responsibility for implementing security and privacy controls, as well as methods for evaluating control effectiveness and efficiency. Roles and responsibilities are carefully structured and appointed making sure that conflicting duties are identified and separated.

Infobip is a cloud services provider (CSP) offering SaaS and PaaS services globally with implemented controls for proper management of security and privacy related risks taking into account geographic location of Customer information, tenant isolation controls, and enabling support for country/regional regulatory requirements. Shared roles and responsibilities are defined in order to clarify the relationship between the Customers and Infobip for information security management.

Information security and privacy policies assign responsibility to upper management for the implementation of information security and privacy controls. Managers are accountable for the correct implementation of information security and privacy controls within their processes, technology, and people. Information security and privacy are integral components for every initiative, program, or project. Information security and privacy controls are designed, implemented, and evaluated during the entire life cycle of any given initiative, program, or project.

Infobip maintains contacts with relevant regulatory institutions, agencies, and telecommunication bodies.

Infobip has formally defined risk management methodology (in line with ISO 31000 and COSO framework) with the purpose to identify and prioritize internal and external threats facing Infobip, and prioritize the most prominent risks based on impact, likelihood, and management's controls.

Risk tolerance level in terms of financial impact is linked to operating profit and risks are described in terms of relation to OKRs (Objectives and Key Results).

Risk ownership has been assigned to individual business units, control functions, as well as on region specific basis.

Risk assessment process is based on likelihood and impact that determine final significance level. Risk treatment is decided depending on the inherent risk score. Risk mitigation strategies and controls that are identified through risk assessment are tracked and reviewed by the assigned owner periodically, at least on semi-annual basis as a part of regular risk reviews. If an action plan for introducing new controls arises during risk assessment process, regular monitoring of plans development is conducted.

Infobip's risk function is responsible for regular reporting of the most significant company risks to the responsible Management Board(s).

Mobile devices and teleworking

Infobip offers its employees different work options that include onsite and remote presence to different degrees. For this reason, remote work is treated in a same way as onsite. Strict technical and security controls are implemented to ensure that our corporate data, and our Customer's data are secured, no matter how it is accessed. Remote access security controls include a secure VPN connection with 2FA authentication for network access and additional 2FA for cloud applications.

To ensure the security of teleworking and the use of mobile devices, company-owned mobile devices (e.g., mobile phones and tablets) are managed using Mobile Device Management (MDM) system, enabling employees to securely access company systems and applications. MDM also provides capabilities to remotely monitor and control mobile devices using work profiles aligned with the business requirements. BYOD is possible for employees who accept enrollment of their private devices to company's MDM.

Access to the production environment and all supporting infrastructure, including Customer information, using mobile devices is not possible.

Human resources security

Infobip People Operations Department is responsible for managing and overseeing the employment process. People Operations Department uses all legally acceptable screening and background verification methods. Employee evaluation and screening are achieved by conducting multiple interviews during the candidate selection process. All candidates must provide proof of their education and/or certification, while other checks are performed in line with applicable labor laws.

All Infobip employees need to acknowledge and formally accept terms and conditions of employment, as well as sign a non-disclosure agreement (NDA) that specifies the obligation of keeping the classified information confidential even after the termination of employment or contractual relationship. Infobip ensures that all employees and third parties handle information in accordance with the required classification level and act according to the Acceptable Use Policy.

Infobip established an internal awareness program using a variety of training methods (e.g., instructor-led training, e-learning, periodic newsletters) and knowledge testing methods, addressing relevant information security, privacy, and compliance topics. All new and existing employees are obliged to periodically attend Awareness training.

Violations of internal policies and procedures may be subject to a disciplinary process.

Asset management

Asset management and protection begin with establishing and maintaining an inventory of assets with correlated roles (e.g. owners, custodians, users) and responsibilities for all assets.

Assets are classified from various perspectives, taking into consideration asset type (i.e., physical, logical, or information assets), asset value and importance, business criticality, implementation environment, and a variety of security and privacy attributes.

Acceptable Use Policy, Information Classification and Handling Policy and associated procedures specify rules for acceptable use and handling of information assets throughout the asset's lifecycle.

Formal procedures and secure disposal mechanisms compliant with NIST Special Publication 800-88, Guidelines for Media Sanitization, are developed and implemented to prevent unauthorized disclosure, or data retrieval from disposed media or deleted data. Procedures address the return and removal of all Customer cloud data and customer-derived data. At the Customer's request, Infobip can issue a written confirmation (i.e. a certificate) that the deletion of the Customer's data is completed.

Access control

Physical and logical access controls ensure that access to information, systems and facilities is based upon business and security requirements. Access is granted upon the least-privilege principle (only minimal set of needed privileges) and need-to-know basis (only minimal access to needed information). Privileged access is restricted and managed through a formal access management approval process.

Access Control Policy sets the access rules specific for facilities, networks, systems, applications, and information, where users are provided only with the access that has been specifically authorized.

Formal processes for user provisioning, registration, and de-registration are in place for all user types, all systems, and services that are part of Infobip information system. Business/asset owners periodically review access rights for all employees and external parties. Access rights of all employees and third parties to information and information processing facilities are removed upon termination of their employment, contract, or agreement, or adjusted upon change.

Users are responsible and are held accountable for safeguarding their authentication information. Secure log-on procedures are implemented where required by the Access control policy. Password systems require interactive login for users. Procedures and technical controls are in place to ensure adequate quality passwords, following the leading practices (e.g., NIST Special Publication 800-63-3, Digital Identity Guidelines).

Digital identity management principles require the usage of personalized and unique user and systems identification ensuring that every interaction with ICT systems is traced to a single entity (e.g., user or system). Different user privilege levels (i.e., standard users and privileged users) may require the usage of additional authentication factors (e.g. software or hardware authentication keys) during the authentication process.

Access to program source code and production environment is restricted and aligned with business, security, and privacy requirements.

Additional information:

- https://www.infobip.com/docs/account-settings#security-settings
- https://www.infobip.com/docs/essentials/manage-users
- https://www.infobip.com/docs/essentials/manage-roles

Cryptography

Cryptographic controls are implemented to ensure the protection of confidentiality, integrity, and authenticity of personally identifiable information (PII) and all other types of sensitive information. Policies regulate the use of appropriate cryptographic controls and the key management processes setting the rules of the use, protection, and lifetime of cryptographic keys and keying material.

Cryptographic key management activities are performed by Infobip Corporate Security Department adhering to all relevant principles and policies.

Infobip supports modern cryptographic algorithms aligned with relevant leading practices in cryptography (such as NIST National Institute of Standards and Technology Special Publication 800-175B Revision 1 Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms). This alignment ensures that information is adequately protected with the most efficient cryptographic controls taking into consideration the state of the information (e.g., in-transit or at-rest) and the system or a system component which processes, transmits or stores information.

For example, Customers using Infobip Platform via API or web-based interface (Portal) will utilize various cryptographic mechanisms which ensure that all transmitted and stored information is protected using modern cryptographic algorithms, following inbound and outbound data flows:

- Encryption in-transit:
    - HTTPS (Hypertext Transfer Protocol Secure) - web interfaces
    - IPSec VPN (Virtual Private Network) – establishment of secure tunnels
    - SMPP (Short Message Peer-to-Peer) over SSL/TLS – secure
    - SFTP (Secure File Transfer Protocol) - secure file transfer
- Encryption at-rest:
    - Message content encryption: AES-256
    - Transparent disk encryption: AES-256
    - Backup archives encryption: AES-256

Physical and environmental security

Infobip implemented physical and environmental security processes and controls to prevent unauthorized physical access and to reduce damage and interference to information and information processing facilities. Information processing facilities (e.g., data centers, offices) represent physical areas that contain Information and communications technology (ICT) equipment and information in digital or physical form. Security perimeters define security areas and their boundaries. Levels of security areas are aligned with the sensitivity or criticality of processed information. Guidelines and procedures specify appropriate practices for working in secure areas.

Infobip uses co-location services and public cloud infrastructure (IaaS) and has outsourced implementation and maintenance of physical and environmental security controls of the locations where Customer data is stored and processed to the service providers. The decision on the appropriate collocation provider is made based on the maturity level of such service provider. Infobip inspects the initial state of the provider and conducts annual reassessments, which may include one or more of the following: inspection of valid certificates and independent audit reports, questionnaires, on-site visits.

Controls for the protection of processing facilities against external and environmental threats and hazards, including power/cabling failures and other disruptions caused by failures in supporting utilities are in place.

Protection controls include security personnel, physical access controls (Controls gates, locks, barriers), video surveillance various methods and mechanisms for protection against external and environmental threats.

Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises are controlled by physical control measures and when possible, isolated from information processing facilities to avoid unauthorized access.

Equipment, information, or software cannot be taken off-site without prior authorization. All equipment containing storage media is validated to confirm that sensitive data and licensed software have been removed, or securely overwritten before disposal.

Clean desk policy for physical documents and removable storage media and clear screen policy for information processing facilities are adopted across the organization.

Operations security

Operational procedures and responsibilities are implemented to ensure correct and secure operations of information processing facilities and successful management of security related risks.

The change management process ensures that all organizational, business processes, information processing changes are controlled and approved. Capacity management ensures that ICT resources are continuously monitored and adjusted to accommodate existing, as well as future requirements. Changes that affect or may affect the Services our Customers are using are communicated publicly in a timely manner containing relevant information (e.g. technical descriptions, impacts, and duration). Customers can subscribe to our status page to get notifications for updates.

Development, testing, and operational environments are segregated to mitigate the risks of unauthorized access or changes to the operational environment. To ensure segregation in virtual computing environments when providing cloud services, logical segregation controls are implemented on various levels, e.g., information, virtualized applications, operating systems, storage, networks to ensure adequate protection of multi-tenant environments.

Security standards define appropriate security measures for each system type (i.e. server, database, network device, application, etc.) taking into consideration the nature of processed, transmitted, or stored information, system attributes, exposure, participation in cloud services, threats, and vulnerabilities. Implementation of standardized security and privacy controls is mandatory before the production release of an ICT component. After the production release, systems and services are continuously monitored, periodically tested to validate the correct operation of security controls.

Additional information:

- https://status.infobip.com/

Anti-malware measures

Technical controls and systems to ensure appropriate malware detection, prevention, and recovery, Anti-malware controls are implemented across Infobip's information system on various technical layers and are combined with educational efforts for increasing awareness of all employees and third parties.

Backup and recovery

Backup copies of information, software, and system images are taken and tested regularly in accordance with backup strategy and related policies. The objective is to ensure protection against the loss of data. Backup policies define the frequency of creating backups, appropriate security controls, and retention periods, taking into consideration the criticality and value of information and recovery point objectives. After the expiry of the backup retention period, information is securely deleted or disposed of.

Backup copies are protected with appropriate control mechanisms (e.g., access controls and cryptographic controls). All relevant backup information (strategy, schedule, methods, and the list of implemented security controls) is available to Customers.

Recovery testing is conducted on at least annual basis to validate the integrity of backed-up information and to verify the duration of the recovery process.

Logging and monitoring

Logging and monitoring processes and systems (multiple systems are in use, including SIEM) ensure the proper recording and generation of evidence related to user activities, exceptions, system and application events, faults, and information security events. Logs are protected against tampering and unauthorized access with special attention to administrator access and operator logs. An audit trail is established for all relevant user-system interactions.

All production systems and applications are in the scope of logging and monitoring, enabling automated event correlation and analysis. Teams of dedicated employees continuously oversee and manage the logging and monitoring systems with capabilities to respond to monitoring alerts taking special consideration to security and privacy context.

Logging and monitoring capabilities are available for SaaS (Software as a Service) and PaaS (Platform as a Service) Customers, providing information regarding the access, usage, and service operations. Several security aspects of cloud services are monitored to ensure that the malicious usage of a platform (e.g., to attack others or to leak data) is detected in a timely manner.

The clocks of all relevant information processing systems or security domains are synchronized to a central reference time source.

The retention period of logging records is kept according to business and regulatory requirements.

Retention of Customer activity and traffic logs may be customized to Customer specific requirements (if they are not contradicting applicable regulation and Infobip's capabilities) and will be subject to additional costs.

Additional information:

- https://www.infobip.com/docs/essentials/account-settings#audit-log
- https://www.infobip.com/docs/analyze

Control of operational software

Control of operational software ensures the integrity of operational systems. Procedures are in place to control the procurement process and the installation of software. Only software which is formally reviewed and approved by the information security personnel is permitted for installation and usage.

Vulnerability management

Information about technical vulnerabilities of information systems is continuously monitored and processed in a timely manner. Exposure to vulnerabilities is evaluated and appropriate measures are taken to address the related risks.

Vulnerability identification methods include the usage of periodic automated vulnerability scanners, penetration testing, bug bounty programs, and gathering of threat intelligence. All production systems and system components are in the scope of the vulnerability management process.

Automated vulnerability scanning is achieved using the best-in-class tools, penetration testing is conducted by experienced independent third-party specialists.

Priority of vulnerability remediation takes into consideration evaluated vulnerability score corresponding to CVSS (Common Vulnerability Scoring System), exploitability, and existing compensating controls.

Remediation methods include patch management process, with all the systems and systems components in the scope, dedicated software development, or implementation of different remediation measures or compensating controls in order to reduce identified risks to acceptable levels. General security risks are also documented through Infobip Enterprise Risk Management (ERM) Program.

Infobip can provide information to Customers regarding the management of technical vulnerabilities related to use services and information.

Network security

Network security management processes and controls ensure the protection of information in networks and supporting information processing facilities. Security mechanisms, service levels of all network services are identified and documented. Networks services and interfaces are grouped taking into consideration their function, sources, and destination of traffic and exposure. Groups are segregated in network segments (e.g. public, DMZ, internal, restricted, etc.) filtered by appropriate network security devices, permitting only allowing approved network traffic matrices.

Transfer of information using any type of communication facilities and channels is protected taking into consideration the nature and risks of each channel.

System acquisition, development, and maintenance

Security requirements of information systems ensure that security and privacy are an integral part of information systems during their entire lifecycle. The requirements for information security controls are included in the business and technical requirements for new information systems or development of existing information systems, taking into consideration all relevant criteria, risk, and sensitivity of a system, with detailed analysis of all publicly exposed systems. Information publicly available via public-facing services are protected from fraudulent activity, modification of information involved incomplete transmission, routing errors, unauthorized message duplication, or message replays.

Principles for engineering secure systems are established, documented, maintained, and applied to any information system development efforts.

Security in development and support processes ensures that information security is designed and implemented from the beginning and through the entire development lifecycle of information systems. Rules for the development of software and systems defined and applied for all developments. Principles for engineering secure systems are documented, maintained, and applied to any information system development. All changes are controlled using formal change control processes and procedures.

Development efforts occur in a separated and protected development environment for all development and integration efforts covering the entire system development lifecycle.

Functional and non-functional acceptance testing programs ensure that all systems are acquired or developed on predefined and testable criteria. Testing also includes manual and automated techniques for validation effectiveness and efficiency of security and privacy controls.

Test data is carefully selected, protected, and controlled from expanding the controls which regulate the separation of development, testing, and operational environments.

Additional information:

- https://infobipengineering.gitbook.io/handbook/how-we-code-and-deploy

Information security incident management

Information security incident management processes ensure consistent, effective, and efficient methodology for treating incidents. Roles and responsibilities and procedures are established to ensure a rapid, effective, and systematic response to information security or privacy-related incidents.

Information security events are reported through appropriate channels as quickly as possible. All employees and external parties' users are required to report any observed or suspected information security weaknesses or deficiencies in systems or services. Information security events are assessed and potentially classified as information security incidents.

Information security incident response is conducted in accordance with the documented procedures. Knowledge gained from managing information security incidents is used to reduce the probability or impact of future incidents. Procedures for identification, collection, acquisition, and preservation of information that may be used as evidence are established.

Dedicated incident response teams are continuously monitoring security events systems and are available for immediate support in case of an incident.

As a global company Infobip has a legislative and/or regulative requirement to report security incidents per applicable local regulation/legislation. Any incident involving client data is firstly communicated to the client and the client is notified in case the information is shared with specific regulator or legislative body as per applicable requirements. Infobip notifies the Customer on confirmed security incidents directly affecting services or data used by the Customers.

Infobip informs external parties (customers, regulatory and legislative bodies) as soon as possible, but no later than 72 hours after the event has been classified as significant security incident and the clear connection with external party's services and data has been established. Means of communication (e-mail, telephone call) is determined by external party preferences.

During security incident handling process, Infobip will update initial notification in case of important facts discovery.

Business continuity management

Information security continuity is always embedded within business continuity management (BCM) to ensure the protection of information and systems and to anticipate and prepare for harmful events.

Continuity and recovery plans are developed to ensure information security and continuity of information security management in adverse situations (e.g., during crisis or disaster). Processes, procedures, and controls are developed and implemented that guarantee the required level of continuity for information security during an adverse situation.

Verification, review, and testing of continuity plans are conducted periodically or in the event of changes in the environment, to ensure that the plans are valid and effective during adverse situations.

Information processing facilities are implemented with redundancy and high availability techniques in order to support availability requirements for all Infobip's services.

Additional information:

- https://www.infobip.com/downloads/ensuring-business-continuity

Compliance

Management of information security and the implementation of related processes, policies, and procedures are independently reviewed at predefined intervals or when significant changes relevant to security and privacy domains occur. Reviews also include an inspection on a technical level assessing the effectiveness and efficiency of technical measures.

To ensure compliance with legislative, regulatory, and contractual requirements, processes for identification and monitoring of applicable legislation and contractual requirements are implemented. Legal and contractual compliance includes the management of the intellectual property.

Legal documentation and related records are protected from loss, destruction, falsification, unauthorized access, and unauthorized release, in accordance with applicable regulatory and business requirements.

Legal requirements related to privacy and protection of personally identifiable (PII) are continuously monitored and implemented.

The usage of cryptographic controls is compliant with all applicable agreements, laws, and regulations.

Infobip is formally certified with:

- ISO/IEC 9001 (Quality Management System),
- ISO/IEC 27001 (Information Security Management System),
- ISO/IEC 27017 (Code of practice for information security controls based on ISO/IEC 27002 for cloud services),
- ISO/IEC 27018 (Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors),
- AICPA SOC2 type I (American Institute of Certified Public Accountants System and Organization Controls 2 - Trust Services Criteria), and
- NCSC (National Cyber Security Centre) Cyber essentials.

Infobip conducts self-evaluation with CSA STAR Level 1 (Cloud Security Alliance Security, Trust, Assurance, and Risk) program and HIPAA (scope limited to standalone SMS service only).

All compliance is assessed on annual basis and certificates are available for download from our web page: https://www.infobip.com/certificates.

At the Customer's request, Infobip can provide summary reports of all aforementioned certification audits. Additionally, Customers can conduct independent reviews as part of their contractual rights.

Abbreviations and acronyms

- AES - Advanced Encryption Standard
- AICPA - American Institute of Certified Public Accountants
- BCM - Business continuity management
- CPaaS - Communications platform a service
- CSA - Cloud Security Alliance
- DMZ - Demilitarized zone
- HTTPS - Hypertext Transfer Protocol Secure
- ICT - Information and Communication Technology
- IEC - International Electrotechnical Commission
- ISMS - Information security
- ISO - International Organization for Standardization
- NCSC - National Cyber Security Centre
- PaaS - Platform as a Service
- PII - Personally identifiable information
- QMS - Quality Management System
- SaaS - Software as a service
- SFTP - Secure File Transfer Protocol
- SMPP - Short Message Peer-to-Peer
- SOC2 - System and Organization Controls 2
- TLS - Transport Layer Encryption
- VPN - Virtual Private Network