Data Security and Privacy Principles
IBM Cloud Services

KUP12494-USEN-01

Contents

Overview

IBM cloud services include infrastructure, platform, and software offerings. Technical and organizational security and privacy measures are implemented for each cloud service in compliance with IBM policy according to its architecture, intended use, and the type of service provided. Figure 1 provides an illustration of the general division of responsibility within each service type.

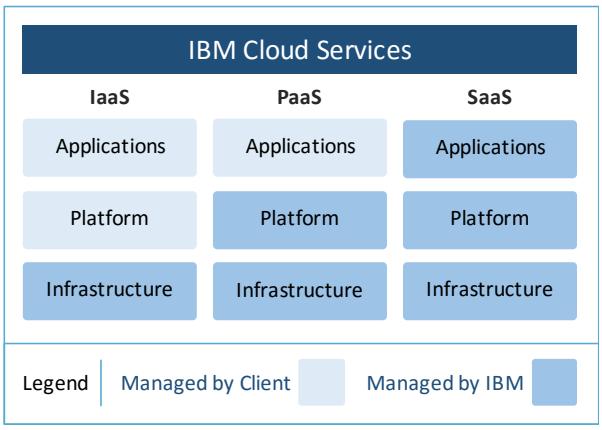

Figure 1: IBM cloud service offering types

IBM Infrastructure as a Service (IaaS) offerings provide computing resources on which clients may deploy and operate software, such as operating systems, runtimes, middleware, and applications of their choice. IaaS clients are responsible for the applications, content, runtimes, middleware, and operating systems they deploy on the IaaS solution, including the implementation and management of data security and privacy measures that are not physical.

IBM Platform as a Service (PaaS) offerings allow clients to create, deploy, and manage cloud applications using systems, networks, storage, runtime frameworks, libraries, and integration and management tools that may be included as a part of the service. PaaS clients manage the applications and content they deploy on the PaaS solution, including the implementation and management of data security and privacy measures for their applications and data.

IBM Software as a Service (SaaS) offerings provide standardized applications from cloud environments for which IBM manages deployment, administration, operation, maintenance, and security of the applications, including underlying middleware, platforms, and infrastructure. SaaS clients continue to manage their end user accounts, appropriate use of the IBM SaaS offering, and the data they process pursuant to the terms of the cloud service agreement. Given their own requirements, SaaS clients are responsible for assessing the suitability of the standard data security and privacy measures that IBM implements.

IBM's specific management responsibilities for each cloud service, regardless of type, are set out in the relevant offering agreement. The data security and privacy measures designed to, among other things, defend IBM cloud services against such risks as accidental loss, unauthorized access, and unauthorized use of client data are set out or incorporated into each service description, including any configurable options and services that may be available.

This Data Security and Privacy Principles document describes the overarching IBM policies and practices that are incorporated into each service description by reference.

Governance

IBM's IT security policies, which derive their authority from specific corporate instructions, are established and managed by the IBM CIO organization and are an integral part of IBM's

business. Compliance with internal IT policies is mandatory and audited.

Security Policies

IBM information security policies are reviewed at least annually and refined as necessary to keep current with modern threats and in line with updates to broadly accepted international standards, such as ISO/IEC 27001 and 27002.

IBM follows a mandated set of employment verification requirements for all new hires, including supplemental employees. These standards also apply to wholly owned subsidiaries and joint ventures. The requirements, which may be subject to change, include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks if the candidate previously worked for a government entity. Each IBM company is responsible for implementing the above requirements in its hiring process as applicable and permissible under local law.

IBM employees are required to complete security and privacy education annually and certify each year that they will comply with IBM's ethical business conduct, confidentiality, and security requirements, as set out in IBM's Business Conduct Guidelines.

Security incidents are handled in accordance with IBM incident management and response policies, taking into account data breach notification requirements under applicable law.

The core functions of IBM's global cybersecurity incident management practice are conducted by IBM's Computer Security Incident Response Team (CSIRT). CSIRT is managed by IBM's Chief Information Security Office and is staffed with global incident managers and forensic analysts. National Institute of Standards and Technology, United States Department of Commerce (NIST) guidelines for computer security incident handling have informed the development and remain the foundation of IBM's global incident management processes.

The CSIRT coordinates with other functions within IBM to investigate suspected incidents, and if warranted, define and execute the appropriate response plan. Upon determining that a security incident has occurred, IBM will promptly notify affected cloud services clients as appropriate.

Access, Intervention, Transfer and Separation Control

The architecture of IBM cloud services maintains logical separation of client data. Internal rules and measures separate data processing, such as inserting, modifying, deleting, and transferring data, according to the contracted purposes. Access to client data, including any personal data, is allowed only by authorized personnel in accordance with principles of segregation of duties, strictly controlled under identity and access management policies, and monitored in accordance with IBM's internal privileged user monitoring and auditing program.

IBM's privileged access authorization is individual, role-based, and subject to regular validation. Access to client data is restricted to the level required to deliver services and support to the client (i.e., least required privilege).

Transfer of data within IBM's network takes place on wired infrastructure and behind firewalls, without the use of wireless networking.

Upon request or service termination, pursuant to the terms of the cloud service agreement, client data is rendered unrecoverable in conformity with NIST guidelines for media sanitization.

Service Integrity and Availability Controls

IBM cloud services undergo penetration testing and vulnerability scanning prior to production release. Additionally, penetration testing, vulnerability scanning, and ethical hacking is performed regularly by IBM and authorized independent third parties.

Modifications to operating system resources and application software are governed by IBM change management policies. Changes to network devices and firewall rules are also governed by the change management policies and are separately reviewed by security staff prior to implementation.

IBM's data center services support a variety of information delivery protocols for transmission of data over public networks, such as HTTPS, SFTP, and FTPS. IBM systematically monitors production data center resources 24x7. Internal and external vulnerability scanning is regularly conducted by authorized administrators to help detect and resolve potential exposures.

Each IBM cloud service has business continuity and disaster recovery plans, which are developed, maintained, verified, and tested in compliance with the ISO 27002 Code of Practice for Information Security Controls. Recovery point and time objectives for each cloud service are established according to its architecture and intended use and provided in the service description or other transaction document. Backup data intended for off-site storage, if any, is encrypted prior to transport.

Security configuration and patch management activities are performed and reviewed regularly. IBM's infrastructure is subject to emergency planning concepts, such as disaster recovery and solid disk mirroring. Business continuity plans for IBM's infrastructure are documented and regularly revalidated.

Activity Logging and Input Control

IBM policy requires administrative access and activity in its cloud services' computing environments to be logged and monitored, and the logs to be archived and retained in compliance with IBM's worldwide records management plan. Changes made to production cloud services are recorded and managed in compliance with IBM change management policy.

Physical Security and Entry Control

IBM maintains physical security standards designed to restrict unauthorized physical access to data center resources. Entry points into IBM data centers are limited, controlled by access readers, and monitored by surveillance cameras. Access is allowed only by authorized personnel.

Delivery areas and loading docks where unauthorized persons may enter the premises are strictly controlled. Deliveries are scheduled in advance and require approval by authorized personnel. Personnel who are not part of the operations, facilities, or security staff are registered upon entering the premises and are escorted by authorized personnel while on the premises.

Terminated employees are removed from the access list and required to surrender their access badges. Use of access badges is logged.

Order Control

Data processing is performed according to offering agreement in which IBM describes the terms, functionality, support, and maintenance of a cloud service offering and measures taken to maintain the confidentiality, integrity, and availability of client data.

Compliance

IBM information security standards and management practices for cloud services are aligned to the ISO/IEC 27001 standard for information security management and comply with the ISO/IEC 27002 Code of Practice for Information Security Controls. Assessments and audits are conducted regularly by IBM to track compliance with its information security standards. Additionally, independent third party industry standard audits are performed annually in all IBM production data centers.

Third Party Subprocessors

IBM cloud services may require third party subprocessors to access client data in normal performance of their contracted duties. If such a third party subprocessor is engaged in the delivery of a cloud service, the subprocessor and its role will be provided upon request. IBM requires all such subprocessors to maintain standards, practices, and policies which preserve the overall level of security and privacy provided by IBM.

Additional Resources

IBM Cloud Services Agreement
http://www.ibm.com/support/operations/files/pdf/csa_us.pdf

IBM Secure Engineering portal
http://www.ibm.com/security/secure-engineering/

IBM Security Vulnerability Management
http://www.ibm.com/security/secure-engineering/process.html

IBM Business Conduct Guidelines
http://www.ibm.com/investor/governance/business-conduct-guidelines.html

A Letter to Our Clients about Government Access to Data
http://asmarterplanet.com/blog/2014/03/open-letter-data.html

IBM SaaS Data Processing Locations
http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=ST&infotype=SA&htmlfid=KUJ12409USEN&attachment=KUJ12409USEN.PDF

IBM Corporation

Route 100

Somers, NY 10589

Produced in the United States of America

April 2016