Data Security and Privacy Principles for IBM Cloud Services

The technical and organizational measures provided in this Data Security and Privacy attachment (DSP) apply to IBM Cloud Services, including any underlying applications, platforms, and infrastructure components operated and managed by IBM in providing the Cloud Service (components), except where Client is responsible for security and privacy and otherwise specified in a transaction document (TD). Client is responsible for: a) determining whether the Cloud Service is suitable for Client's use and; b) implementing and managing security and privacy measures for elements not provided and managed by IBM within the Cloud Service described in applicable Attachments and TDs (such as systems and applications built or deployed by Client upon an Infrastructure as a Service offering, or Client end-user access control to Software as a Service offerings). The measures implemented and maintained by IBM within each Cloud Service will be subject to annual certification of compliance with ISO 27001 or SSAE SOC 2 or both.

1. Data Protection

a. Security and privacy measures for each Cloud Service are designed in accordance with IBM's secure engineering and privacy-by-design practices to protect Content input into a Cloud Service, and to maintain the availability of such Content pursuant to the Agreement, including applicable Attachments and TDs. Client is the sole controller for any personal data included in the Content and appoints IBM as a processor to process such personal data (as those terms are defined in Regulation (EU) 2016/679, General Data Protection Regulation). IBM will treat all Content as confidential by not disclosing Content except to IBM employees, contractors, and subprocessors, and only to the extent necessary to deliver the Cloud Service, unless otherwise specified in a TD.

b. IBM will securely sanitize physical media intended for reuse prior to such reuse, and will destroy physical media not intended for reuse, consistent with National Institute of Standards and Technology, United States Department of Commerce (NIST), guidelines for media sanitization.

c. Upon request, IBM will provide evidence of stated compliance and accreditation, such as certificates, attestations, or reports resulting from accredited independent third-party audits, such as ISO 27001, SSAE SOC 2, and other industry standards as specified in a TD. Where applicable, the accredited independent third-party audits will occur at the frequency required by the relevant standard to maintain the Cloud Service's stated compliance and accreditation.

d. Additional security and privacy information specific to a Cloud Service may be available in the relevant TD or other standard documentation to aide in Client's initial and ongoing assessment of a Cloud Service's suitability for use. Such information may include evidence of stated certifications and accreditations, information related to such certifications and accreditations, data sheets, FAQs, and other generally available documentation. IBM will direct Client to available standard documentation if asked to complete Client-preferred questionnaires or forms and Client agrees such documentation will be utilized in lieu of any such request. IBM may charge an additional fee to complete any Client-preferred questionnaires or forms or to provide consultation to Client for such purposes.

2. Security Policies

a. IBM will maintain and follow IT security policies and practices that are integral to IBM's business and mandatory for all IBM employees. The IBM CIO will maintain responsibility and executive oversight for such policies, including formal governance and revision management, employee education, and compliance enforcement.

b. IBM will review its IT security policies at least annually and amend such policies as IBM deems reasonable to maintain protection of Cloud Services and Content processed therein.

c. IBM will maintain and follow its standard mandatory employment verification requirements for all new hires and will extend such requirements to wholly owned IBM subsidiaries. In accordance with IBM internal process and procedures, these requirements will be periodically reviewed and include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks as deemed necessary by IBM. Each IBM company is responsible for implementing these requirements in its hiring process as applicable and permitted under local law.

d. IBM employees will complete security and privacy education annually and certify each year that they will comply with IBM's ethical business conduct, confidentiality, and security policies, as set out in IBM's Business Conduct Guidelines. Additional policy and process training will be provided to persons granted administrative access to Cloud Service components that is specific to their role within IBM's operation and support of the Cloud Service, and as required to maintain compliance and certifications stated in the relevant TD.

3. Security Incidents

a. IBM will maintain and follow documented incident response policies consistent with NIST guidelines for computer security incident handling and will comply with data breach notification terms of the Agreement.

b. IBM will investigate unauthorized access and unauthorized use of Content of which IBM becomes aware (security incident), and, within the Cloud Service scope, IBM will define and execute an appropriate response plan. Client may notify IBM of a suspected vulnerability or incident by submitting a technical support request.

c. IBM will notify Client without undue delay upon confirmation of a security incident that is known or reasonably suspected by IBM to affect Client. IBM will provide Client with reasonably requested information about such security incident and the status of any IBM remediation and restoration activities.

4. Physical Security and Entry Control

a. IBM will maintain appropriate physical entry controls, such as barriers, card-controlled entry points, surveillance cameras, and manned reception desks, to protect against unauthorized entry into IBM facilities used to host the Cloud Service (data centers). Auxiliary entry points into data centers, such as delivery areas and loading docks, will be controlled and isolated from computing resources.

b. Access to data centers and controlled areas within data centers will be limited by job role and subject to authorized approval. Use of an access badge to enter a data center and controlled areas will be logged, and such logs will be retained for not less than one year. IBM will revoke access to controlled data center areas upon separation of an authorized employee. IBM will follow formal documented separation procedures that include, but are not limited to, prompt removal from access control lists and surrender of physical access badges.

c. Any person duly granted temporary permission to enter a data center facility or a controlled area within a data center will be registered upon entering the premises, must provide proof of identity upon registration, and will be escorted by authorized personnel. Any temporary authorization to enter, including deliveries, will be scheduled in advance and require approval by authorized personnel.

d. IBM will take precautions to protect the Cloud Service's physical infrastructure against environmental threats, both naturally occurring and man-made, such as excessive ambient temperature, fire, flood, humidity, theft, and vandalism.

5. Access, Intervention, Transfer and Separation Control

a. IBM will maintain documented security architecture of networks managed by IBM in its operation of the Cloud Service. IBM will separately review such network architecture, including measures designed to prevent unauthorized network connections to systems, applications and network devices, for compliance with its secure segmentation, isolation, and defense-in-depth standards prior to implementation. IBM may use wireless networking technology in its maintenance and support of the Cloud Service and associated components. Such wireless networks, if any, will be encrypted and require secure authentication and will not provide direct access to Cloud Service networks. Cloud Service networks do not use wireless networking technology.

b. IBM will maintain measures for a Cloud Service that are designed to logically separate and prevent Content from being exposed to or accessed by unauthorized persons. IBM will maintain appropriate isolation of its production and non-production environments, and, if Content is transferred to a non-production environment, for example in order to reproduce an error at Client's request, security and privacy protections in the non-production environment will be equivalent to those in production.

c. To the extent described in the relevant TD, IBM will encrypt Content not intended for public or unauthenticated viewing when transferring Content over public networks and enable use of a cryptographic protocol, such as HTTPS, SFTP, and FTPS, for Client's secure transfer of Content to and from the Cloud Service over public networks.

d. IBM will encrypt Content at rest when specified in a TD. If the Cloud Service includes management of cryptographic keys, IBM will maintain documented procedures for secure key generation, issuance, distribution, storage, rotation, revocation, recovery, backup, destruction, access, and use.

e. If IBM requires access to Content, it will restrict such access to the minimum level required. Such access, including administrative access to any underlying components (privileged access), will be individual, role-based, and subject to approval and regular validation by authorized IBM personnel following the principles of segregation of duties. IBM will maintain measures to identify and remove redundant and dormant accounts with privileged access and will promptly revoke such access upon the account owner's separation or the request of authorized IBM personnel, such as the account owner's manager.

f. Consistent with industry standard practices, and to the extent natively supported by each component managed by IBM within the Cloud Service, IBM will maintain technical measures enforcing timeout of inactive sessions, lockout of accounts after multiple sequential failed login attempts, strong password or passphrase authentication, and measures requiring secure transfer and storage of such passwords and passphrases.

g. IBM will monitor use of privileged access and maintain security information and event management measures designed to: a) identify unauthorized access and activity; b) facilitate a timely and appropriate response; and c) enable internal and independent third-party audits of compliance with documented IBM policy.

h. Logs in which privileged access and activity are recorded will be retained in compliance with IBM's worldwide records management plan. IBM will maintain measures designed to protect against unauthorized access, modification, and accidental or deliberate destruction of such logs.

i. To the extent supported by native device or operating system functionality, IBM will maintain computing protections for its end-user systems that include, but may not be limited to, endpoint firewalls, full disk encryption, signature-based malware detection and removal, time-based screen locks, and endpoint management solutions that enforce security configuration and patching requirements.

6. Service Integrity and Availability Control

a. IBM will: a) perform security and privacy risk assessments of its Cloud Services at least annually; b) perform penetration testing and vulnerability assessments, including automated system and application security scanning and manual ethical hacking, before production release and annually thereafter; c) enlist a qualified independent third-party to perform penetration testing at least annually; d) perform automated management and routine verification of underlying components' compliance with security configuration requirements; and e) remediate identified vulnerabilities or noncompliance with its security

configuration requirements based on associated risk, exploitability, and impact. IBM will take reasonable steps to avoid Cloud Service disruption when performing its tests, assessments, scans, and execution of remediation activities.

b. IBM will maintain policies and procedures designed to manage risks associated with the application of changes to its Cloud Services. Prior to implementation, changes to a Cloud Service, including its systems, networks, and underlying components, will be documented in a registered change request that includes a description and reason for the change, implementation details and schedule, a risk statement addressing impact to the Cloud Service and its clients, expected outcome, rollback plan, and documented approval by authorized personnel.

c. IBM will maintain an inventory of all information technology assets used in its operation of the Cloud Service. IBM will continuously monitor and manage the health, including capacity, and availability of the Cloud Service and underlying components.

d. Each Cloud Service will be separately assessed for business continuity and disaster recovery requirements pursuant to documented risk management guidelines. Each IBM Cloud Service will have, to the extent warranted by such risk assessment, separately defined, documented, maintained, and annually validated business continuity and disaster recovery plans consistent with industry standard practices. Recovery point and time objectives for the Cloud Service, if provided, will be established with consideration given to the Cloud Service's architecture and intended use, and will be described in the relevant TD. Physical media intended for off-site storage, if any, such as media containing Cloud Service backup files, will be encrypted prior to transport.

e. IBM will maintain measures designed to assess, test, and apply security advisory patches to the Cloud Service and its associated systems, networks, applications, and underlying components within the Cloud Service scope. Upon determining that a security advisory patch is applicable and appropriate, IBM will implement the patch pursuant to documented severity and risk assessment guidelines. Implementation of security advisory patches will be subject to IBM change management policy.