IBM Data Security and Privacy Principles

1. Definitions

Capitalized terms used herein have the meanings given below or if not defined below, the meanings given in the applicable written contract between IBM and Client for the IBM Services.

Client – is the entity to which IBM is providing the IBM Services under an IBM Services Document.

Components – are the application, platform, or infrastructure elements of an IBM Service that IBM operates and manages.

Content – consists of all data, software, and information that Client or its authorized users provide, authorize access to, or input to IBM Services.

DSP – is this IBM Data Security and Privacy Principles document.

IBM Cloud Services – are "as a service" IBM offerings that IBM makes available via a network, such as software as a service, platform as a service, or infrastructure as a service.

IBM Services Document – is a Transaction Document and any other document that is incorporated into a written contract between IBM and a Client and that addresses details of a specific IBM Service.

IBM Services – are (a) IBM Cloud Services, (b) other IBM service offerings, including infrastructure or application service offerings that IBM delivers and dedicates to or customizes for a Client, and (c) any other services, including consulting, maintenance, or support, that IBM provides to a Client.

Security Incident – is an unauthorized access and unauthorized use of Content.

Transaction Document – is a document that details the specifics of transactions, such as charges and a description of and information about an IBM Cloud Service. Examples of Transaction Documents include statements of work, service descriptions, ordering documents and invoices for an IBM Cloud Service. There may be more than one Transaction Document applicable to a transaction.

2. Overview

The technical and organizational measures provided in this DSP apply to IBM Services (including any Components) only where IBM has expressly agreed to comply with the DSP in a written contract between IBM and Client. For clarity, those measures do not apply where Client is responsible for security and privacy or as specified below or in an IBM Services Document.

a. Client is responsible for determining whether an IBM Service is suitable for Client's use and implementing and managing security and privacy measures for components that IBM does not provide or manage within the IBM Services. Examples of Client responsibilities for IBM Services include: (1) the security of systems and applications built or deployed by the Client upon an infrastructure as a service or platform as a service offering or upon infrastructure, Components or software that IBM manages for a Client, and (2) Client end-user access control and application level security configuration for a software as a service offering that IBM manages for a Client or an application service offering that IBM delivers to a Client.

b. Client acknowledges that IBM may modify this DSP from time to time at IBM's sole discretion and such modifications will replace prior versions as of the date that IBM publishes the modified version. Notwithstanding anything to the contrary in any written contract between IBM and Client, the intent of any modification will be to: (1) improve or clarify existing commitments, (2) enable IBM to appropriately prioritize its security focus to address evolving data and cybersecurity threats and issues, (3) maintain alignment to current adopted standards and applicable laws, or (4) provide additional features and functionality. Modifications will not degrade the security or data protection features or functionality of IBM Services.

c. In the event of any conflict between this DSP and an IBM Services Document, the IBM Services Document will prevail and if the conflicting terms are in a Transaction Document, they will be identified as overriding the terms of this DSP and will only apply to the specific transaction.

3. Data Protection

a. IBM will treat all Content as confidential by not disclosing Content except to IBM employees, contractors, and suppliers (including subprocessors), and only to the extent necessary to deliver the IBM Services.

b. Security and privacy measures for each IBM Service are implemented in accordance with IBM's security and privacy by design practices to protect Content processed by an IBM Service, and to maintain the availability of such Content pursuant to the applicable written contract between IBM and Client, including applicable IBM Services Documents.

c. Additional security and privacy information specific to an IBM Service may be available in the relevant IBM Services Document or other standard documentation to aid in Client's initial and ongoing assessment of an IBM Service's suitability for Client's 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 security or privacy questionnaires.

4. Security Policies

a. IBM will maintain and follow written IT security policies and practices that are integral to IBM's business and mandatory for all IBM employees. The IBM Chief Information Security Officer 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 IBM Services and Content.

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 processes 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 IBM's 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 training will be provided to any persons granted privileged access to Components that is specific to their role within IBM's operation and support of the IBM Services, and as required to maintain compliance and accreditations stated in any relevant IBM Services Document.

5. Compliance

a. For standard (non-custom) IBM Cloud Services, the measures implemented and maintained by IBM within each IBM Cloud Service will be subject to annual certification of compliance with ISO 27001 or SSAE SOC 2, or both, unless stated otherwise in an IBM Services Document.

b. Additionally, IBM will maintain compliance and accreditation for the IBM Services as defined in an IBM Services Document.

c. Upon request, IBM will provide evidence of the compliance and accreditation required by 5a. and 5b., such as certificates, attestations, or reports resulting from accredited independent third-party audits (accredited independent third-party audits will occur at the frequency required by the relevant standard).

d. IBM is responsible for these data security and privacy measures even if IBM uses a contractor or supplier (including subprocessors) in the delivery or support of an IBM Service.

6. Security Incidents

a. IBM will maintain and follow documented incident response policies consistent with National Institute of Standards and Technology, United States Department of Commerce (NIST) guidelines or equivalent industry standards for computer security incident handling and will comply with the data breach notification terms of the applicable written contract between IBM and Client.

b. IBM will investigate Security Incidents of which IBM becomes aware, and, within the scope of the IBM Services, IBM will define and execute an appropriate response plan. Client may notify IBM of a suspected vulnerability or incident by submitting a request through the incident reporting process specific to the IBM Service (as referenced in an IBM Services Document) or, in the absence of such process, 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.

7. 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 managed facilities (data centers) used to host the IBM Services. Auxiliary entry points into such data centers, such as delivery areas and loading docks, will be controlled and isolated from computing resources.

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

c. Any person granted temporary permission to enter an IBM-managed data center facility or a controlled area within such 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 physical infrastructure of IBM managed data center facilities against environmental threats, both naturally occurring and man-made, such as excessive ambient temperature, fire, flood, humidity, theft, and vandalism.

8. Access, Intervention, Transfer and Separation Control

a. IBM will maintain a documented security architecture for Components. IBM will separately review such security 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.

b. IBM may use wireless networking technology in its maintenance and support of the IBM Services and associated Components. Such wireless networks, if any, will be encrypted and require secure authentication and will not provide direct access to IBM Cloud Services networks. IBM Cloud Services networks do not use wireless networking technology.

c. IBM will maintain measures for an IBM 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 to reproduce an error at Client's request, security and privacy protections in the non-production environment will be equivalent to those in production.

d. 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, or FTPS, for Client's secure transfer of Content to and from the IBM Services over public networks.

e. IBM will encrypt Content at rest if and as specified in an IBM Services Document. If an IBM 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.

f. If IBM requires access to Content to provide the IBM Services, and if such access is managed by IBM, IBM will restrict 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 upon the request of authorized IBM personnel, such as the account owner's manager.

g. Consistent with industry standard practices, and to the extent natively supported by each Component, IBM will maintain technical measures enforcing timeout of inactive sessions, lockout of

accounts after multiple sequential failed login attempts, strong password or passphrase authentication, password change frequency, and secure transfer and storage of such passwords and passphrases.

h. IBM will monitor use of privileged access and maintain security information and event management measures designed to: (1) identify unauthorized access and activity, (2) facilitate a timely and appropriate response, and (3) enable internal and independent third-party audits of compliance with documented IBM policy.

i. 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.

j. 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.

k. IBM will securely sanitize physical media intended for reuse prior to such reuse, and will destroy physical media not intended for reuse, consistent with NIST guidelines for media sanitization.

9. Service Integrity and Availability Control

a. IBM will: (1) perform security and privacy risk assessments of the IBM Services at least annually, (2) perform security testing and vulnerability assessments of the IBM Services before production release and at least annually thereafter, (3) enlist a qualified independent third party, IBM X-Force™ or, if specified in an IBM Services Document, another qualified testing service to perform penetration testing of the IBM Cloud Services, at least annually, (4) perform automated vulnerability scanning of underlying Components of the IBM Services against industry security configuration best practices, (5) remediate identified vulnerabilities from security testing and scanning, based on associated risk, exploitability, and impact, and (6) take reasonable steps to avoid disruption to the IBM Services when performing its tests, assessments, scans, and execution of remediation activities.

b. IBM will maintain measures designed to assess, test, and apply security advisory patches to the IBM Services and associated systems, networks, applications, and underlying Components within the scope of the IBM Services. Upon determining that a security advisory patch is applicable and appropriate, IBM will implement the patch pursuant to documented severity and risk assessment guidelines, based on Common Vulnerability Scoring System ratings of patches, when available. Implementation of security advisory patches will be subject to IBM change management policy.

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

d. IBM will maintain an inventory of all information technology assets used in its operation of IBM Services. IBM will continuously monitor and manage the health, including capacity, and availability of IBM Services and underlying Components.

e. Each IBM Service will be separately assessed for business continuity and disaster recovery requirements through appropriate business impact analysis and risk assessments intended to identify and prioritize critical business functions. Each IBM Service will have, to the extent warranted by such risk assessments, separately defined, documented, maintained, and annually validated business continuity and disaster recovery plans consistent with industry standard practices. Recovery point and time objectives for an IBM Service, if provided for in the relevant IBM Services Document, will be established with consideration given to the IBM Service's architecture and intended use. Physical media intended for off-site storage, if any, such as media containing backup files, will be encrypted prior to transport.