Kyndryl Data Security and Privacy Principles

kyndryl

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 Kyndryl and Client for the Kyndryl Services.

Client – is the entity to which Kyndryl is providing the Kyndryl Services under a Kyndryl Services Document.

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

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

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

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

Kyndryl Services – are (a) Kyndryl service offerings, including infrastructure or application service offerings that Kyndryl delivers and dedicates to or customizes for a Client, and b) any other services, including consulting, maintenance, or support, that Kyndryl 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 a Kyndryl Service. Examples of Transaction Documents include statements of work, service descriptions, ordering documents and invoices for a Kyndryl 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 Kyndryl Services (including any Components) only where Kyndryl has expressly agreed to comply with the DSP in a written contract between Kyndryl and Client. For clarity, those measures do not apply where Client is responsible for security and privacy or as specified below or in a Kyndryl Services Document.

a. Client is responsible for determining whether a Kyndryl Service is suitable for Client's use and implementing and managing security and privacy measures for components that Kyndryl does not provide or manage within the Kyndryl Services. Examples of Client responsibilities for Kyndryl 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 Kyndryl manages for a Client, and (2) Client end-user access control and application level security configuration for a software as a service offering that Kyndryl manages for a Client or an application service offering that Kyndryl delivers to a Client.

b. Client acknowledges that Kyndryl may modify this DSP from time to time at Kyndryl's sole discretion and such modifications will replace prior versions as of the date that Kyndryl publishes the modified version. Notwithstanding anything to the contrary in any written contract between Kyndryl and Client, the intent of any modification will be to: (1) improve or clarify existing commitments, (2) enable Kyndryl 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 Kyndryl Services.

c. In the event of any conflict between this DSP and a Kyndryl Services Document, the Kyndryl 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. Kyndryl will treat all Content as confidential by not disclosing Content except to Kyndryl employees, contractors, and suppliers (including subprocessors), and only to the extent necessary to deliver the Kyndryl Services.

b. Security and privacy measures for each Kyndryl Service are implemented in accordance with Kyndryl's security and privacy by design practices to protect Content processed by a Kyndryl Service,

and to maintain the availability of such Content pursuant to the applicable written contract between Kyndryl and Client, including applicable Kyndryl Services Documents.

c. Additional security and privacy information specific to a Kyndryl Service may be available in the relevant Kyndryl Services Document or other standard documentation to aid in Client's initial and ongoing assessment of a Kyndryl 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. Kyndryl will direct Client to available standard documentation if asked to complete Client-preferred security or privacy questionnaires.

4. Security Policies

a. Kyndryl will maintain and follow written IT security policies and practices that are integral to Kyndryl's business and mandatory for all Kyndryl employees. The Kyndryl 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. Kyndryl will review its IT security policies at least annually and amend such policies as Kyndryl deems reasonable to maintain protection of Kyndryl Services and Content.

c. Kyndryl will maintain and follow its standard mandatory employment verification requirements for all new hires and will extend such requirements to wholly-owned Kyndryl subsidiaries. In accordance with Kyndryl 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 Kyndryl. Each Kyndryl company is responsible for implementing these requirements in its hiring process as applicable and permitted under local law.

d. Kyndryl employees will complete Kyndryl's security and privacy education annually and certify each year that they will comply with Kyndryl's ethical business conduct, confidentiality, and security policies, as set out in Kyndryl's Business Conduct Guidelines. Additional training will be provided to any persons granted privileged access to Components that is specific to their role within Kyndryl's operation and support of the Kyndryl Services, and as required to maintain compliance and accreditations stated in any relevant Kyndryl Services Document.

5. Compliance

a. Kyndryl will maintain compliance and accreditation for the Kyndryl Services as defined in a Kyndryl Services Document.

b. Upon request, Kyndryl will provide evidence of the compliance and accreditation required by 5a., 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).

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

6. Security Incidents

a. Kyndryl 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 Kyndryl and Client.

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

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

7. Physical Security and Entry Control

a. Kyndryl 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 Kyndryl managed facilities (data centers) used to host the Kyndryl 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 Kyndryl-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. Kyndryl will revoke access to Kyndryl-managed data centers upon separation of an authorized employee. Kyndryl 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 a Kyndryl-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. Kyndryl will take precautions to protect the physical infrastructure of Kyndryl 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. Kyndryl will review the security architecture for Components, including measures 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. Kyndryl may use wireless networking technology in its maintenance and support of the Kyndryl Services and associated Components. Such wireless networks, if any, will be encrypted and require secure authentication.

c. Kyndryl will maintain measures for a Kyndryl Service that are designed to logically separate and prevent Content from being exposed to or accessed by unauthorized persons. Kyndryl 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. Kyndryl 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 Kyndryl Services over public networks.

e. Kyndryl will encrypt Content at rest if and as specified in a Kyndryl Services Document. If a Kyndryl Service includes management of cryptographic keys, Kyndryl will maintain documented procedures for secure key generation, issuance, distribution, storage, rotation, revocation, recovery, backup, destruction, access, and use.

f. If Kyndryl requires access to Content to provide the Kyndryl Services, and if such access is managed by Kyndryl, Kyndryl 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 Kyndryl personnel following the principles of segregation of duties. Kyndryl 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 Kyndryl personnel, such as the account owner's manager.

g. Consistent with industry standard practices, and to the extent natively supported by each Component, Kyndryl 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. Kyndryl 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 Kyndryl policy.

i. Logs in which privileged access and activity are recorded will be retained in compliance with Kyndryl's policy. Kyndryl 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, Kyndryl will maintain computing protections for its end-user systems that include, but may not be limited to, endpoint firewalls, full disk encryption, malware detection and removal, time-based screen locks, and endpoint management solutions that enforce security configuration and patching requirements.

k. Kyndryl 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. Kyndryl will: (1) perform security and privacy risk assessments of the Kyndryl Services at least annually, (2) perform security testing and vulnerability assessments of the Kyndryl Services before production release and at least annually thereafter**,** (3) perform penetration testing on capabilities and offerings before production release and annually thereafter, (4) perform automated vulnerability scanning of underlying Components of the Kyndryl 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 Kyndryl Services when performing its tests, assessments, scans, and execution of remediation activities.

b. Kyndryl will maintain measures designed to assess, test, and apply security advisory patches to the Kyndryl Services and associated systems, networks, applications, and underlying Components within the scope of the Kyndryl Services. Upon determining that a security advisory patch is applicable and appropriate, Kyndryl 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 Kyndryl change management policy.

c. Kyndryl will maintain policies and procedures designed to manage risks associated with the application of changes to Kyndryl Services. Prior to implementation, changes to a Kyndryl 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 Kyndryl Service and its clients, expected outcome, rollback plan, and documented approval by authorized personnel.

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

e. Each Kyndryl 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 Kyndryl 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 a Kyndryl Service, if provided for in the relevant Kyndryl Services Document, will be established with consideration given to the Kyndryl 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.