Data Retention Policy

Purpose and Scope:

- This data retention policy defines the organization's objectives and requirements for data retention.

- This policy covers all data within the organization’s custody or control, regardless of the medium the data is stored in (electronic form, paper form, etc.) Within this policy, the medium that holds data is referred to as information, no matter its form.

- This policy applies to all users of information systems within the organization. This typically includes employees, contractors, and any external parties that come into contact with systems and information the organization owns or controls (hereinafter referred to as “users”). This policy must be made readily available to all users.

Background:

- The organization is bound by multiple legal, regulatory, and contractual obligations regarding the data it retains. These obligations stipulate how long data can be retained and how data must be destroyed. Examples of legal, regulatory, and contractual obligations include laws and regulations in the local jurisdiction where the organization conducts business and contracts made with employees, customers, service providers, partners, and others.

- The organization may also be involved in events such as litigation or disaster recovery scenarios requiring access to original information to protect the organization’s interests or those of its employees, customers, service providers, partners, and others. As a result, the organization may need to archive and store information for longer than it may be needed for day-to-day operations.

Policy:

Information Retention

- Retention is defined as the maintenance of information in a production or live environment that an authorized user can access in the ordinary course of business.

- Information used in the development, staging, and testing of systems shall not be retained beyond their active use period nor copied into production or live environments.

- By default, the information retention period shall be an active use period of exactly two years from its creation unless an exception permits a longer or shorter retention period. The business unit responsible for the information must request the exception.

- After the active use period of information is over by this policy and approved exceptions, information must be archived for a defined period. Once the defined archive period is over, the information must be destroyed.

- Each business unit is responsible for the information it creates, uses, stores, processes, and destroys, according to the requirements of this policy. The responsible business unit is considered to be the information owner.

- The organization's legal counsel may issue a litigation hold to request that information relating to potential or actual litigation, arbitration, or other claims, demands, disputes, or regulatory action be retained by instructions from the legal counsel.

- Each employee and contractor affiliated with the company must return information in their possession or control to the organization upon separation and/or retirement.

- Information owners must enforce the retention, archiving, and destruction of information, and communicate these periods to relevant parties.

Information Archiving

- Archiving is defined as the secured storage of information such that the information is rendered inaccessible by authorized users in the ordinary course of

business but can be retrieved by an administrator designated by company management.

- The default archiving period of information shall be 7 years unless an approved exception permits a longer or shorter period. Exceptions must be requested by the information owner.

- The information must be destroyed (defined below) at the end of the elapsed archiving period.

Information Destruction

- Destruction is defined as the physical or technical destruction sufficient to render the information contained in the document irretrievable by ordinary commercially-available means.

- The organization must maintain and enforce a detailed list of approved destruction methods appropriate for each type of information archived, whether in physical storage media such as CD-ROMs, DVDs, backup tapes, hard drives, mobile devices, portable drives, or in database records or backup files. Physical information in paper form must be shredded using an authorized shredding device; waste must be periodically removed by approved personnel.

Retention and archival periods for information that is created, processed, stored, and used by the organization are defined internally.

ENFORCEMENT

We expect all employees to comply with this policy and any related policies, standards, processes, procedures, and guidelines. Failure and/or refusal to abide by this policy may be deemed a violation. Compliance with the policies will be a matter of periodic review by the Information security officer / Information Security Team. Any employee found to have violated this policy may be subject to disciplinary action, as deemed appropriate by management and Human Resources policies.

- **Monitoring:** The company employs appropriate technology solutions to monitor policy/ procedure compliance.

- **Self-Assessment:** The CEO/CTO are required to conduct self-assessment within their areas of control to verify compliance with this policy/ procedure.

- **Security Audits:** Internal Audit may assess the implementation of and compliance with this policy/ procedure as part of its audit program.

SPECIAL CIRCUMSTANCES AND EXCEPTIONS

All exceptions to this policy/ procedure will require a waiver explicitly approved by one of Our Organisation's CEO/CTO.