Number: STR/DPRR/V.1.1/2025-26

Title: Data Privacy & Record Retention Policy

	NAME	TITLE	SIGNATURE	DATE
Author	**Sachin Garg**	**AVP**		
Reviewer/	**Shaurya Malhotra**	**VP – IT & TECH**		**18th Jul 2025**
Authoriser	**Shaurya Malhotra**	**VP – IT & TECH**		**16th Jul 2025**

Effective Date:	**12th Nov 2025**
Review Date:	**12th Nov 2026**

Change History

SOP no.	Effective Date	Significant Changes	Previous SOP no.
1.0	08-Sep-2023	Adoption of Policy	NA
1.1	12-Nov-2025	Renewal of the policy	NA

1. Purpose

To ensure storage and retention of information, data and records as per contractual and legal requirements and protection from loss, falsification, destruction, unauthorized access and unauthorized release.

2. Scope

The scope of this policy is applicable to all information, data and records, whether in electronic or non-electronic form, which are created, stored, retained, exchanged and disposed by **Stride One Capital Private Limited** Herein referred as **StrideOne**.

Responsibilities

- The primary ownership of implementing this policy is with All Departments and Teams handling Data and Records
- The ISG shall implement this Procedure under guidance of Leadership Team and in coordination with Department Heads.

3. Policy

a) Identification and Classification of Data and Records

- All Departments shall identify the data and records which are created or handled by them.
- All data and records, which belong to Customers, External Person, Entity or Organization shall also be identified under External Origin Data or Records.
- Organizational Classification shall be applied to all types of Data and Records as below. For more details refer concerned Policy / Procedure are per reference section.
    - Confidential
    - Internal Use
    - Public
    - External Origin

- All types of data and records, existing within **StrideOne**, shall be identified and documented within prescribed format along with Custodian information and classification applied to the same. (*Ref: Data and Records Register*)

b) Retention Period of Data and Records

- The retention period for each type of data and record shall be defined and applied by the concerned Department who creates or handles the data or record.
- While deciding the retention period, following sequence shall be followed –
    - Check Statutory or Regulatory or Legislative requirement of retention for each type of Data or Record,
    - Check if any Contractual requirement exists for retention of each type of data or record,
    - Check Organizational policy about retention of data or records,
    - Select the highest applicable retention period and apply to concerned data or record.
- In case of externally provided data or records, which are provided by an external person or entity, the retention period as specified by external person or entity shall be referred in addition to the above listed sequence.
- The retention period defined and applied for each type of data and record shall also be applied to the backups / archival of concerned data or record.
- Electronic and Non-electronic data and records shall be appropriately archived during the retention period.
- The retention period, once applied to any data or record, shall not be changed without prior approval from InfoSec Team.
- The retention period, for all types of data and records within **StrideOne**, shall be defined and documented in prescribed format.

c) Protection of Data and Records

- Access to each type of Data or Record shall be provided basis classification applied to such data or record.
- The access provision and revocation to all types of data and records shall be governed by corresponding policies as listed in the Reference section.
- Risks for electronic and non-electronic data and records shall be assessed and mitigation controls shall be put in place to protect the data and records.
- Physical (non-electronic) data and records shall be protected from loss or damage. Environmental and natural factors such as fire, water, corrosion, pests etc. shall be considered while applying controls for protection. Similarly, man-made disasters such as theft, misplacement, destruction etc. shall also be considered while applying protection.
- Electronic data and records shall be protected from unauthorized access, theft, disclosure, corruption, changes, destruction etc. Adequate provisions about backup and redundancy of data and records shall be made in case of disasters.

d) Disposal of Data and Records

- Data and records, when no longer required or at the end of retention period, shall be destroyed or disposed securely to avoid any unauthorized access.
- All non-electronic (physical) data and records shall be destroyed using paper shredders and the trash shall be carefully disposed.
- All electronic data and records shall be disposed / destroyed using secure controls such as –
    - Degaussing or Physical Destruction of Hard Disks
    - Physical destruction of Tapes
    - Physical destruction of Optical Storage Disks, Flash Drives etc.
    - Delete + Purge of Electronic Data and Records
    - In case of rented or leased systems, secure wiping / formatting of Hard Disks and Medias before returning back

- Wherever the data and records are provided or originated from an external person or entity, the same shall either be returned back to the originator at the end of retention period or destroyed using secure methods as mentioned above.
- The destruction or disposal of data or records shall also be applied to backup or archived copies at the end of retention period.
- Records of destruction / disposal of Personal Data / PII / Confidential Information shall be retained by concerned Department for future audits and reference.