****

**Data Retention and Destruction Policy Template**

*By Paul Kirvan, FBCI, CISA*

|  |
| --- |
| **Title:** Data Retention and Destruction Policy  |
| **Department:**  | **Version:** Original |
| **Approved by:** | **Approval Date:**  |
| **Senior Management Approval:** |
| **Effective Date:** | **Last Updated:** |
| **Author:** |
| **Scope**This policy applies to the <specify location> of <company name> <enter address> |
| **Authority** This policy is hereby approved and authorized.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Signature Title Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Signature Title Date \_\_\_\_\_\_\_\_\_\_\_\_ |
| **Purpose** The purpose of this policy is to define the activities associated with the development, updating and deployment of data retention and destruction plans and procedures that protect <company name> information systems, networks, data, databases and other information assets. Additional policies governing data management activities will be addressed separately. Additional purposes for this plan include compliance with applicable standards and regulations governing data retention and destruction, and compliance with environmental, sustainability and related regulations.  |
| **Scope**The scope of this data retention and destruction policy is all information technology systems, software, databases, applications and network resources needed by the Company to conduct its business. The policy is applicable to all Company employees, contractors and other authorized third-party organizations. |
| **Statement of Compliance**This policy is designed to be compliant with the U.S. Data Protection Act of 1998, Freedom of Information Act of 2000, Fair and Accurate Credit Transactions Act of 2003 (FACTA), Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, Gramm-Leach-Bliley Act (GLBA), the European Union's General Data Protection Regulation (GDPR), ISO 27040: Information Technology -- Security techniques -- Storage security, and NIST SP 800-209 -- Security Guidelines for Storage Infrastructure.Data retention and destruction policy compliance is managed by the IT department, with support from <company name> department leadership and subject matter experts. To achieve compliance, data retention and destruction programs must include appropriate procedures, and identify staffing and technology resources to meet compliance requirements. Compliance verification (especially for data destruction) is performed monthly by the IT department, internal audit or other appropriate entity.  |
| **Policy**The Information Technology (IT) department is responsible for managing all data retention and destruction activities for the Company. Other departments, such as Finance and Accounting, Operations and Human Resources, are also responsible for providing the IT department with their requirements for data retention and destruction. The IT department is responsible for developing, executing and periodically testing data retention and destruction procedures. The IT department also acknowledges it will comply with appropriate industry standards for data retention and destruction in its activities. 1. The company shall develop comprehensive data retention and destruction plans in accordance with good data management practices as defined by established standards.
2. Data retention and destruction activities shall be performed as part of the company’s data management program, which administers and manages the overall technology data management program, which includes:
	* Planning and design of data retention and destruction activities.
	* Identification of data retention and destruction teams, defining their roles and responsibilities and ensuring they are properly trained and prepared to perform their duties.
	* Planning, design and documentation of data retention and destruction plans.
	* Scheduling of updates to data retention and destruction risk analyses.
	* Planning and delivery of awareness and training activities for employees and data retention and destruction team members.
	* Planning and execution of data retention and destruction plan exercises.
	* Designing and implementing data retention and destruction maintenance activities to ensure that plans are up to date and ready for use.
	* Ensuring that data retention and destruction procedures are consistent with the Company’s environment and sustainability management programs.
	* Preparing for management review and auditing of data retention and destruction plan(s).
	* Planning and implementation of continuous improvement activities for data retention and destruction activities and plans.
3. Formal risk assessments (RA) and business impact analyses (BIA) shall include requirements for data retention and destruction activities; RAs and BIAs shall be updated at least annually to ensure they are in alignment with the business and its technology requirements.
4. Data retention and destruction plans and schedules shall address electronic data stored on electronic media such as CDs, hard disk drives, solid state drives, magnetic tape and other approved media.
5. Data retention and destruction plans and schedules shall address data stored on non-electronic media (e.g., paper files, microfiche).
6. Data retention and destruction plans and schedules shall address electronic information systems (e.g., servers, routers, switches) and components (e.g., cabling and connectors, power supplies, storage racks) and other assets that are currently out of production or scheduled to be phased out of production environments.
7. Data retention plans and schedules shall establish the storage requirements and associated metrics (e.g., length of storage, type of storage media) for electronic and non-electronic information as well as systems supporting the IT infrastructure.
8. Data destruction plans and schedules shall establish the parameters for destruction of electronic data (e.g., overwriting, reformatting, degaussing, firmware-based erasure, physical data media destruction), non-electronic data (e.g., shredding of hard copy), and systems and components (e.g., third-party destruction services).
9. Data retention and destruction plans and schedules shall be periodically reviewed and tested in a suitable environment to ensure that data, databases, media, systems and other relevant elements can be retained or destroyed and that <company name> management and employees understand how the plans and schedules are to be executed as well as their roles and responsibilities.
10. Data retention and destruction plans and schedules will be consistent with environmental and sustainability programs the Company has established.
11. All employees must be made aware of the data retention and destruction program and their own roles and responsibilities.
12. Data retention and destruction plans and other documents are to be kept up to date and will reflect existing and changing circumstances.
 |
| **Data Retention and Destruction Specifications** Following are specific data retention and destruction technical requirements:**General**1. State the frequency and types of data/system retention activities to be performed.
2. State the frequency and types of data/system destruction activities to be performed.
3. State the schedule for data retention and destruction activities.
4. State who (e.g., internal staff, outside third parties) is responsible for data retention and destruction.
5. State who should be notified if a problem with retention and destruction activities is identified.

**Data/System Retention Procedures** 1. State how data (e.g., electronic and non-electronic) is stored and retained.
2. State how systems are stored and retained.
3. State the schedule for data retention activities.
4. State where data/systems are stored and retained.
5. State process for ensuring that retention procedures work properly.
6. State process for validation of data/media retention.
7. State process for complying with Company environmental and sustainability programs.

**Data/System Destruction Procedures**1. State data destruction metrics and time frames.
2. State process for data/system destruction.
3. State process for validation of data/media destruction.
4. State the schedule for data destruction activities.
5. State process for complying with Company environmental and sustainability programs.

**Retention and Destruction Requests**1. State process for processing requests for data restoration and destruction.
 |
| **Policy Leadership** **<Title of executive>** is designated as the corporate owner responsible for data/system retention and destruction activities for the Company. Resolution of issues in the support of data/system retention and destruction activities should be coordinated with IT management and others as needed.  |
| **Policy Responsibilities*** Policy Approval – The **<title of executive>** is responsible for approving this policy.
* Policy Implementation – The <enter name of department or individual> is responsible for planning, organizing and implementing all activities that fulfill this policy.
* Policy Maintenance and Updating – The <enter name of department or individual> is responsible for all activities associated with maintaining and updating this policy.
* Policy Compliance – The <enter name of department or individual> is responsible for ensuring compliance with relevant standards, regulations and good practice for data retention and destruction.
* Policy Compliance with environmental management programs – The <enter name of department or individual> is responsible for ensuring compliance with Company policies and programs for environmental and sustainability management.
* Policy Monitoring, Review and Audit – The <enter name of department or individual> is responsible for monitoring and reviewing this policy and providing support for scheduled audits – both internally and externally executed – on data retention and destruction activities.
* Policy Improvement – The <enter name of department or individual> is responsible for defining and implementing activities that will improve this policy.
 |
| **Management Review**<Enter name of department or individual> will review and update this data retention and destruction policy on an annual basis. As changes to this policy are indicated in the course of business, <enter name of department or individual> may initiate a change management process to update this policy.  |
| **Policy Enforcement**The **<title of executive>** will enforce this policy.  |
| **Penalties for Non-Compliance** In situations where it is determined that data retention and destruction activities do not comply with this policy, the IT department team assigned to this activity will prepare a report stating the reason(s) for non-compliance and present it to IT management for resolution. Failure to comply with this data retention and destruction policy within the allotted time for resolution may result in verbal reprimands, notes in personnel files, termination, and such other remedies as deemed appropriate.  |
| **Policy Location**The policy will be signed, scanned into an electronic file and posted in the following location on the network: <enter location of policy> |