****

**IT Data Storage Policy**

|  |
| --- |
| **Title:** ITData StoragePolicy |
| **Department:** IT | **Version:** Original |
| **Approved by:** | **Approval Date:**  |
| **Senior Management Approval:** |
| **Effective Date:** | **Last Updated:** |
| **Author:** |
| **Scope**This policy applies to <company> employees, contractors, consultants, temporary workers and all other individuals storing, using or accessing <company> data and information, whether in electronic or hard copy formats.This policy applies to data storage activities that are on premises, as well as remotely managed using cloud-based or company-managed storage technology. |
| **Responsibility**The <company> IT department is responsible for maintaining and updating this policy with the approval of the chief information officer or chief technology officer. |
| **Objectives**The objective of this policy is to define how data – both electronic and hard-copy – will be stored in such a way to protect it, and ensure its security and availability, in accordance with established data management policy and in compliance with applicable laws, standards and good practice.  |
| **Purpose** <The company's> purpose for data storage is to ensure that all data and information – in electronic or hard-copy form – needed by <company> in the performance of its work are stored in a secure repository when not in current use or when archived for future use, such that they are available when needed, are accessible and usable by <company> staff, and are maintained in secure, protected environments until they are retrieved for use, archived or destroyed. The focus of data storage management is to meet the legal requirements for record retention and privacy protection, optimize the use of space, minimize the cost of record retention, and destroy outdated records. |
| **Policy**<Company> requires that its data and information – whether in electronic or hard-copy formats – are stored in a secure manner and be managed so that the company: 1. Meets legal standards for data storage, retrieval and protection
2. Establishes procedures for data storage activities, delivers them to all employees, provides training on the policy as part of the new employee onboarding, provides refresher training as needed, and reviews and updates the procedures as needed
3. Protects the data privacy of employees, customers and others as required by law
4. Optimizes the use of primary data storage facilities to facilitate the timely and secure retrieval of data from storage when needed
5. Establishes rules for the use of employee-owned storage devices and monitors that usage
6. Addresses security issues associated with data storage on company-owned facilities and third-party managed storage services, as well as employee-owned storage devices, to minimize the potential for unauthorized access to company data and information
7. Plans for and budgets for data storage technology, whether on site or remote
8. Regularly reviews and adjusts its data storage facilities – both on site and remote – to promptly accommodate changes in storage requirements

<Company> may designate an employee to serve as data storage manager; this employee is most likely to be part of the IT department. <Company> departments that generate data and information are responsible for establishing appropriate data storage requirements in coordination with the <company> data storage manager. Each department's administrative manager or a designee must: 1. Be familiar with <company's> data storage policy
2. Develop the department's and/or office's data storage requirements, consistent with this policy
3. Educate staff within the department so they understand data storage practices
4. Define storage requirements for confidential data and information

**Confidentiality Requirement** Some <company> data and information may contain nonpublic confidential data. Such data and information are protected by federal, state and local statutes, including the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act and others. In addition to statutory requirements, any confidential data should be stored in accordance with <the company's> privacy and security policies. **Electronically Stored Information** <Company> depends onthe use and availability of electronically stored information (ESI). The ease with which ESI may be created, the technology where ESI may be stored, and rules regarding the use of ESI in litigation all require that <company> manages its data storage activities efficiently and consistent with its legal obligations. Accordingly, all departments must include ESI in the development of their data storage requirements. **Non-Electronic Information Storage**<Company> stores important hard-copy documents in secure, fire-protected storage containers, whether located on site or in secure remote storage facilities. The point at which such information is to be placed into storage and the type of storage to be used are determined by the document's user(s), in collaboration with the data storage manager and/or records manager. **Storage of Data and Information Relevant to Legal Matters** Any data record and other information that is relevant to any pending or anticipated litigation, claim, audit, agency charge, investigation or enforcement action shall be securely stored and retained at least until final resolution of the matter. In these circumstances, the <company> general counsel will notify relevant departments and work with staff to identify and store records (including electronic records) and other information that could be relevant to the litigation. Employees who become aware that an investigation or legal proceeding has commenced or is anticipated against their department or unit promptly must notify their <company> department leadership and/or general counsel so that all records with potential relevance to the investigation or legal proceeding can be stored as necessary. **Disposal and Destruction of Stored Data and Information** The company's data retention policy and/or records management policy will govern the circumstances under which stored data and information can be disposed of and destroyed.  |
| **Enforcement**<Company> employees, vendors and others who do not comply with this policy and the procedures that may be developed from it are subject to possible disciplinary measures including termination of employment as may be determined by <company's> senior management, department leadership, chief information officer and/or human resources departments.  |
| **Management Review**<Company's> executives will review and update policies on an annual basis, or more frequently when changes are authorized. As changes to <company> policies are indicated in the course of business, <company> management may launch a change management initiative to change them. All <company> policies will be available for review in the course of scheduled audits.  |