|  |  |  |
| --- | --- | --- |
| Document ID  **ITSD103** | Title  **IT MEDIA STORAGE** | Print Date  **mm/dd/yyyy** |
| Revision  **0.0** | Prepared By  **Preparer’s Name / Title** | Date Prepared  **mm/dd/yyyy** |
| Effective Date  **mm/dd/yyyy** | Reviewed By  **Reviewer’s Name / Title** | Date Reviewed  **mm/dd/yyyy** |
|  | Approved By  **Final Approver’s Name / Title** | Date Approved  **mm/dd/yyyy** |

**Policy:** To ensure adequate protection and proper handling of Company data and Information Technology storage media.

**Purpose:** To establish controls and procedures for storage, protection, access, procurement and destruction of Company data, Information Technology storage media, and related software; to plan for cost-effective storage technologies that offer long asset life and scalability; and to ensure data integrity and availability.

**Scope:** This procedure applies to all Company data stored by the Information Technology Department, regardless of storage medium.

### Responsibilities:

Information Technology Managers are responsible for developing and reviewing the Company’s data storage plan.

The Information Technology Storage Librarian is responsible for implementing the Company data storage plan.

**Definitions:** Network-attached storage (NAS) – Hard disk storage set up with its own network address rather than being attached to the department computer serving applications to a network’s workstation users.

RAID - Redundant Array of Independent Disks is a method of storing the same data in different places (thus, redundantly) on multiple hard disks.

Storage-area network (SAN) - A high-speed, special-purpose network or subnetwork connecting different kinds of Information Technology storage devices with data servers on behalf of a large network of users.

Storage media – In computers, a storage medium is any technology (including devices and materials) used to place, keep, and retrieve data. The term “storage medium” usually refers to secondary storage, such as that on a hard disk or tape.

**Procedure:**

## IT STORAGE PLANNING

* 1. Information Technology Managers shall oversee development and implementation of an Information Storage Plan that:
     + Ensures data availability, confidentiality, and integrity;
     + Enables rapid and full recovery from natural or manmade disasters;
     + Ensures Company compliance with industry standards and/or legal & regulatory requirements for data storage; and
     + Allows efficient, cost-effective data management.
  2. To develop the Company’s Information Storage Plan, Information Technology Managers shall:
  + Conduct a needs analysis – determine the Company’s storage capacity and requirements by conducting a historical analysis of storage use and reviewing user satisfaction surveys, in accordance with ITAD110 IT DEPARTMENT SATISFACTION and ITAM102 IT ASSET MANAGEMENT;
  + Research and benchmark Information Technology industry practices and standards; and
  + Account for pertinent legal/regulatory requirements (see References A – D).
  1. Information Technology Managers shall design the Information Storage Plan, with the assistance of the Information Technology Storage Librarian.
  2. Information Technology Managers shall submit the Information Storage Plan to Top Management for its review and approval.
  3. Upon approval of the Plan, Information Technology Managers shall communicate the Plan to the Information Technology Storage Librarian and shall arrange for training, as needed.

1. **IT STORAGE PLAN**
   1. Data stores (databases, etc.) shall be uniquely identified, as shall their owners (departments/parties with primary responsibility for generating and updating information).
   2. Data stores shall be identified as mission-critical or not and shall be assigned security levels, indicating whether access shall be restricted, in accordance with ITSD106 IT ACCESS CONTROL.
   3. All data stores shall be backed up according to a set schedule and type. Data shall be retained and disposed of in accordance with ITAD102 IT RECORDS MANAGEMENT.
   4. Backed-up data shall be subjected to a periodic recovery test, in accordance with ITSD104 IT DISASTER RECOVERY.
   5. The Information Technology Storage Librarian shall be responsible for implementing the Information Storage Plan, monitoring storage use, and periodically submitting a status report on information storage to Information Technology Managers.
   * The Information Technology Storage Librarian shall receive vendor training in the event of new storage technologies being implemented.
2. **IT STORAGE PLAN REVIEW**
   1. Information Technology Managers shall periodically (annually, at a minimum) meet with the Information Technology Storage Librarian to review the Information Storage Plan and determine its continuing suitability and conformity to Company requirements and to ensure that data are retrievable and not in danger of loss due to technology changes.

The Information Technology Storage Librarian shall report on changes in Information Technology industry practices, standards, and technologies that have occurred since the most recent review, for possible incorporation into the Plan.

* 1. An external audit of the Company’s Information Storage Plan and processes should be conducted no less than once every three years.
  2. Information Technology Managers shall review the results of such audits and reviews, incorporate them into the Information Technology Storage Plan as needed, and communicate the changes to the Information Technology Storage Librarian.

1. **UPDATING THE IT STORAGE PLAN**
   1. The Information Technology Storage Librarian shall implement required changes to the Information Technology Storage Plan.

4.2 Within a month of such changes being implemented, Information Technology Managers shall conduct a review with the Information Technology Storage Librarian to verify implementation of changes and verify that the desired results were achieved.

**Forms:**

* ITSD103-1 INFORMATION STORAGE PLAN

**References:**

**A.** **NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA) RETENTION AND ACCESS REQUIREMENTS FOR RECORDS (36 CFR 1210.53)**

Federal retention requirements for non-profits are specified in the Code of Federal Regulations (36 CFR 1210.53), which are published by the Office of the Federal Register, National Archives and Records Administration, and may be purchased from the U.S. Government Printing Office (GPO) in Washington, DC.

### B. IRS PROCEDURE 98-25 – RECORDS RETENTION

The U.S. Tax Code requires that, except for farmers and wage-earners, anyone subject to income tax or any person required to file an information return with respect to income must keep such books and records, including inventories, as are sufficient to establish the amount of gross income, deductions, credits, or other matters reported. The books or records required by must be kept available at all times for inspection by authorized internal revenue officers or employees and must be retained so long as the contents thereof may become material in the administration of any internal revenue law.

Note: Section 6.01 requires taxpayers to maintain and make available documentation of the business processes that (1) create the retained records, (2) modify and maintain its records, (3) satisfy the requirements of section 5.01(2) of the procedure and verify the correctness of the taxpayer’s return, and (4) evidence the authenticity and integrity of the taxpayer’s records.

Section 6.02 sets forth four elements that the documentation required under section 6.01 must establish: (1) the flow of data through the system, (2) internal controls that ensure accurate processing, (3) internal controls that prevent unauthorized record changes, and (4) charts of account.

Section 6.03 sets forth six specific types of documentation for each retained file: (1) record formats, (2) field definitions, (3) file descriptions, (4) evidence that periodic checks are undertaken to ensure that data remains accessible, (5) evidence that the records reconcile to the taxpayer’s books, and (6) evidence that the records reconcile to the taxpayer’s return.

1. **SARBANES-OXLEY ACT OF 2002**

The Sarbanes-Oxley Act, enacted by the U.S. Congress in July 2002, created new standards for corporate accountability and new penalties for acts of wrongdoing. Sarbanes-Oxley, or SOX, holds corporate executive officers responsible for financial reporting, mandates internal control processes, and outlaws changing or destroying financial records. SOX also sets forth new records retention guidelines for corporations; in particular, section 802 of the Act pertains to criminal penalties for alteration or destruction of documents.

1. **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)**

Regarding the subject of records storage, the Health Insurance Portability and Accountability Act (HIPAA), enacted by the U.S. Congress in 1996, does not specify storage requirements. The Act is, however, designed to allow patients access to their information, *however or wherever* it is stored.

1. **ISO STANDARD 27002:2013 – INFORMATION TECHNOLOGY-CODE OF PRACTICE FOR INFORMATION SECURITY CONTROL, CLAUSE 12.1.3 (SAFEGUARDING OF ORGANIZATIONAL RECORDS)**

For more, see <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297>.

**Additional Resources:**

1. The Storage Networking Industry Association (SNIA) is a registered 501-C6 non-profit trade association. See <http://www.snia.org/home> for more information on this organization.
2. American Institute of Certified Public Accountants (AICPA) Filing and Record Retention Procedures Guide. See <http://www.aicpa.org> for further information.

**Revision History:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Description of Changes** | **Requested By** |
| 0 | mm/dd/yyyy | Initial Release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

[This page intentionally left blank]

**ITSD103-1 INFORMATION STORAGE PLAN**

Data store name:

Data store ID:

Department:

Responsible party / owner:

Key source of information

(information is mission-critical): 🞏 Y 🞏 N

Purpose: 🞏 Daily usage 🞏 Archival 🞏 Backup & recovery

A. Security level (1=all may access / 5=restricted to owner, IT Security, auditors):

1. Backup schedule / frequency:
2. Backup type (full / partial / incremental):
3. Storage medium (disk, tape, SAN, NAS, etc.):
   * Expected useful life of medium:
4. Retention period:
5. Data disposal (archived data only)

* Method of disposal:

G. Recovery testing (date):

IT Management: Date:

IT Storage Librarian: Date:

[This page intentionally left blank]