Data Storage and Retention Policy

Reviewed By: Reid Tattersall

Date: 06/23/2020

I. Introduction

All data will be stored, backed-up, archived and disposed of in a manner consistent with its sensitivity, requirements and best practices. Data classification is a key component for making consistent and appropriate decisions related to data storage and retention.

Unneeded non-authoritative data (duplicate copies, outdated records, non-business-related files, test data) accumulate in operational locations need to be removed when no longer needed. Purging not only saves IT resources, but also avoids the possibility of compromising sensitive data in these sources that may not be as well protected as the authoritative masters.

II. Purpose

The purpose of this policy is to direct the implementation of standards and procedures for storing, archiving, and disposing of data.

III. IT Policy Common Provisions Apply

IT Policy Common Provisions, policy 1.1, apply to this specific policy, unless otherwise noted.

IV. Roles and Responsibilities

Records Retention Specialist

The functional Records Retention Specialist keeps abreast of record retention requirements and advise functional and technical areas about those requirements.

Security Assurance

Security Assurance reviews and evaluates functional areas for compliance with documented policies and procedures.

V. Specific Provisions

1. Data on Protected Storage

- Data classified as Restricted and Protected Confidential will be stored only in approved locations and on approved equipment or storage facilities.
- BACKNINE INSURANCE AND FINANCIAL SERVICES, INC. employees will refrain from making duplicate copies or shadow files of authoritative data resources.
- Temporary duplicate copies of electronic data created for legitimate reasons must be protected in a like manner to the authoritative data, and removed in a timely manner.
- Standards for storing electronic data containing sensitive data will be created and periodically reviewed.
- Standards for storing hardcopy containing sensitive data will be created and periodically reviewed.
- Periodic reviews will be performed by Security Assurance to ensure compliance with data management policies, standards and procedures.

2. Data Backups and Off-site Storage

- All data located on BACKNINE INSURANCE AND FINANCIAL SERVICES, INC.-owned IT Resources will be backed-up on a regular basis consistent with data classification standards applicable to the data being backed-up.
- Backups of any BACKNINE INSURANCE AND FINANCIAL SERVICES, INC. data whose loss would impact the operation or viability of the BACKNINE INSURANCE AND FINANCIAL SERVICES, INC. will be taken off-site or written off-site to a secure location in a timely manner.
- Any backup media containing DCL3 data taken off-site or backup data sent off-site will be encrypted.

3. Data Storage

- The need to retain data in locations will be reviewed on an ongoing basis.
- Data no longer needed for routine operations, but which must be retained, will be archived in a timely manner.
- The Information Security Program Office (ISPO) in collaboration with Data stewards will develop criteria for deciding when data can be archived.
- ISPO in collaboration with Data stewards will develop procedures for archiving of data.

4. Data Retention

- Data Stewards and Data Managers will be knowledgeable about standards, and procedures regarding retention of data.
- ISPO in collaboration with Record Retention Specialists will develop procedures to ensure that required data is always accessible, especially as backup media ages,

previously supported media is discontinued, supported data formats and standards change, and security controls change.

5. Data Disposal

- The need to retain operational and archived data will be reviewed on an ongoing basis.
- Data no longer needed for routine operations and which need not be retained in archive will be destroyed in a timely manner in compliance with record retention policies.
- Archived data which need no longer be retained will be destroyed in a timely manner in compliance with record retention policies.
- ISPO in collaboration with functional Record Retention Specialists will develop procedures for disposing of data in compliance with record retention schedules.