Data Protection, Storage, and Recovery Policy

1.0 Purpose

The purpose of this policy is to establish guidelines and requirements for the protection, storage, retention, and recovery of the organization's data assets. This policy aims to safeguard sensitive and critical information from unauthorized access, disclosure, modification, loss, or destruction, ensuring data integrity, confidentiality, and availability. It also outlines procedures for preventing data loss and recovering data effectively in the event of an incident.

2.0 Scope

This policy applies to all employees, contractors, consultants, temporary staff, and other agents of the organization who create, access, manage, store, transmit, or dispose of organizational data, regardless of the format (electronic or physical) or location (on-premises or cloud-based). It covers all types of organizational data, including but not limited to customer information, financial records, employee data, intellectual property, and operational data.

3.0 Policy Statements

The following statements outline the specific requirements and guidelines governing data protection, storage, prevention, and recovery within the organization:

3.1 Data Classification

Organizational data must be classified according to its sensitivity and criticality (e.g., Public, Internal, Confidential, Restricted). Data classification levels determine the required security controls for protection, storage, access, and disposal. Detailed data classification guidelines will be maintained separately and made available to relevant personnel.

3.2 Data Protection Measures

*   **Access Control:** Access to data shall be granted based on the principle of least privilege, ensuring users have access only to the information necessary to perform their job functions. Robust authentication mechanisms must be employed.
*   **Encryption:** Sensitive and confidential data must be encrypted both at rest (when stored) and in transit (when transmitted over networks), using organization-approved encryption standards and tools.
*   **Endpoint Security:** All endpoints (desktops, laptops, mobile devices) accessing

organizational data must have approved security software installed and maintained, including anti-malware protection and firewalls, where applicable.
*   **Secure Data Transfer:** Transferring sensitive or confidential data must be done using secure, approved methods (e.g., encrypted email, secure file transfer protocols).
*   **Physical Security:** Physical access to areas where data is stored or processed (e.g., server rooms, file storage areas) must be restricted to authorized personnel.

3.3 Data Storage

*   **Approved Locations:** Organizational data must be stored only on approved systems and platforms (e.g., designated network servers, sanctioned cloud storage services). Storing sensitive or confidential data on personal devices, removable media (unless encrypted and approved), or unauthorized third-party cloud services is prohibited.
*   **Data Minimization:** Only necessary data should be collected and retained. Data should not be stored longer than required for legitimate business or legal purposes.
*   **Secure Disposal:** Data must be disposed of securely when no longer needed, following established procedures that ensure irreversible destruction or deletion, especially for sensitive information and physical media.

3.4 Data Loss Prevention (DLP)

The organization will implement technical and administrative controls to prevent accidental or malicious data loss or exfiltration. This may include DLP software solutions, email content filtering, regular security awareness training for users, and adherence to acceptable use policies. Users are responsible for handling data carefully and reporting any suspected policy violations or security risks.

3.5 Data Backup

*   **Regular Backups:** Critical organizational data must be backed up regularly according to a defined schedule based on data criticality and recovery objectives.
*   **Backup Storage:** Backup copies must be stored securely, with at least one copy maintained in an offsite location to protect against local disasters. Backup media must be protected with appropriate security controls (e.g., encryption, physical security).
*   **Backup Verification:** Backup procedures must include regular testing to verify the integrity of the backups and the ability to restore data successfully.

3.6 Data Recovery

*   **Recovery Procedures:** Documented procedures must be in place for restoring data from backups in the event of data loss, system failure, or disaster. These procedures should align with the organization's Disaster Recovery and Business Continuity Plans.
*   **Recovery Objectives:** Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) should be defined for critical systems and data, guiding backup frequency and recovery priorities.
*   **Incident Response:** Data recovery efforts will be initiated as part of the overall incident response process following a data loss event.

4.0 Roles and Responsibilities

*   **IT Department / Designated Authority:** Responsible for implementing and managing technical controls (security systems, backups, storage infrastructure), developing detailed procedures, and overseeing policy compliance.
*   **Data Owners/Sponsors:** Responsible for classifying data within their purview, defining access requirements, and ensuring appropriate handling according to this policy.
*   **Users:** Responsible for adhering to this policy in their daily work, handling data securely, using approved systems, and reporting incidents or concerns promptly.

5.0 Compliance

5.1 Compliance Measurement

Adherence to this policy will be monitored through various methods, including system audits, security assessments, reviews of access logs, and internal/external audits. The IT Department or designated compliance team (potentially including external partners like Precision Computer where applicable for managed services) will assist in verification activities.

5.2 Exceptions

Any exception to this policy must be formally documented, justified, approved by designated management or the IT Department/Security Team in advance, and regularly reviewed.

5.3 Enforcement

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract termination for third parties, consistent with organizational procedures and applicable regulations.

6.0 Policy Review

This policy shall be reviewed at least annually, or more frequently as needed due to changes in technology, regulations, or business requirements, and updated accordingly.

Revision #2
Created 1 May 2025 17:28:06 by Travis Woolery
Updated 16 September 2025 22:10:08 by Travis Woolery