Standard Operating Procedure (SOP): IT and Security Policy

Owner: IFC - IT Department
Date Created: 04/04/2025
Version: 1.0

1. Introduction

This SOP outlines the structured approach for implementing, maintaining, and reviewing critical IT and security policies within the organization. Each policy is designed to ensure data integrity, operational continuity, risk management, and compliance with relevant regulations. This document details the purpose of each policy, why it is essential, the steps for implementation, and the frequency of review and updates.

2. Policy Framework

2.1 Written Information Security Program (WISP)

WISP is a comprehensive policy that outlines the organization's approach to safeguarding sensitive data. It covers administrative, technical, and physical safeguards to protect against data breaches and unauthorized access.

1. Why?

- To comply with regulations such as IRS 4557, GLBA, and other data protection laws.
- To provide clear guidelines for managing and protecting confidential information.
- To reduce the risk of data loss, theft, or misuse.

2. Policy Update Frequency:

- Reviewed annually or when new threats emerge.

2.2 Backup Policy

The Backup Policy outlines the procedures for data backup, storage, recovery, and management to ensure the availability and integrity of critical business data.

1. Why?

- To prevent data loss due to system failures, cyberattacks, accidental deletion, or hardware malfunctions.
- To ensure business continuity by maintaining access to important data.
- To comply with legal requirements related to data retention and protection.

2. Backup Frequency:

- **Daily Backups:**
    - Use OneDrive's version history to automatically track changes and create daily recovery points.
    - Configure critical systems to perform automated daily backups, including both full and incremental backups, ensuring data is regularly preserved.
- **Weekly Backups:**
    - Weekly snapshots of critical data are automatically generated and securely exported to cloud repositories.
- **Monthly Backups:**
    - At the end of each month, comprehensive data exports are performed and stored in a secondary cloud repository for seven years to ensure compliance with IRS retention requirements.

3. Policy Update Frequency:

- Reviewed annually or after significant data changes.

2.3 Business Continuity and Disaster Recovery (BCDR) Policy

The BCDR Policy provides a framework for maintaining operations during disruptive events, including natural disasters, cyber incidents, and equipment failures.

1. Why?

- To minimize operational downtime and financial loss.
- To ensure the availability of critical business functions during crises.
- To meet legal and contractual obligations regarding continuity planning.

2. Testing BCDR Policy:

- Conduct annual regular BC/DR drills, including simulated disasters.
- Train staff on their roles and responsibilities during a crisis.
- Document lessons learned and update the plan accordingly.

3. Update Frequency:

- Reviewed biannually or after each significant incident.

2.4 Incident Response Policy

This policy provides a structured methodology for identifying, managing, and mitigating cybersecurity incidents.

1. Why?

- To limit damage during security breaches.
- To ensure rapid response to cyber threats.
- To comply with legal obligations related to incident reporting.

2. Policy Update Frequency:

- Reviewed annually or after major incidents.

2.5 Risk Management Policy

This policy outlines the procedures for identifying, assessing, mitigating, and monitoring IT risks.

1. Why?

- To proactively address risks that could affect operations.
- To comply with regulatory standards for risk management.

2. Policy Update Frequency:

- Reviewed annually or when new risks are identified.

2.6 Vendor & Third-Party Risk Management (TPRM) Policy

The TPRM Policy defines the processes for assessing, managing, and mitigating risks associated with third-party vendors and service providers who have access to the organization's IT systems or data.

1. Why?

- To minimize risks associated with outsourcing or using external services.
- To ensure that third-party practices align with the organization's security standards.
- To maintain compliance with data protection regulations and industry standards.

2. Policy Update Frequency:

- Reviewed annually or when onboarding new vendors.

2.7 Privacy Policy

The Privacy Policy outlines how the organization collects, stores, processes, and protects personal data belonging to clients, employees, and partners.

1. Why?

- To comply with privacy regulations such as GDPR, CCPA, and GLBA.
- To maintain customer trust by demonstrating commitment to data protection.
- To define the responsibilities of staff members handling personal data.

2. Update Frequency:

- Reviewed upon significant regulatory changes.

3. Remaining IT and Security Policies

- **Access Control Policy**: Defines how access to systems, applications, and data is granted, modified, and revoked.
- **Acceptable Use Policy (AUP):** Outlines acceptable and unacceptable use of organizational IT resources.
- **Data Classification and Handling Policy:** Describes how data is categorized based on sensitivity and how each category must be handled.

- **Network Security Policy:** Details measures to protect the network from internal and external threats (e.g., firewalls, segmentation).
- **Password Management Policy:** Sets standards for password complexity, rotation, and storage.
- **Data Retention and Destruction Policy:** Defines how long different types of data are retained and how they should be securely disposed of.
- **Encryption Policy:** Details when and how encryption should be used for data at rest and in transit.
- **Patch Management Policy:** Provides guidelines for updating and patching software, systems, and devices to reduce vulnerabilities.
- **Physical Security Policy:** Addresses how physical access to critical systems and data centers is controlled and monitored.

4. Conclusion

Effective IT and security policies are crucial for protecting the organization’s data and ensuring compliance. Regular updates and proper implementation help mitigate risks and maintain a secure working environment. Adhering to these policies supports the organization's commitment to data protection and security.