Information Technology Policy Manual

Table of Contents

1. Purpose and Scope

This Information Technology (IT) Policy Manual outlines the policies and procedures for managing IT systems and assets to ensure efficient, secure, and compliant operations. It applies to all employees, contractors, and third-party vendors who interact with the company's IT systems, including but not limited to hardware, software, networks, and data.

2. Backup and Disaster Recovery Policy

2.1 Purpose

This policy ensures that company data and critical systems are regularly backed up and can be recovered in the event of a disaster, minimizing downtime and data loss.

2.2 Backup Policy

1. Frequency: All critical data and systems must be backed up at least daily. Non-critical data can be backed up weekly.
2. Storage: Backups should be stored in multiple locations, including on-site for quick recovery and off-site or in the cloud for disaster recovery.
3. Retention: Backups must be retained for a minimum of 90 days. Older backups may be archived for compliance or regulatory purposes.
4. Testing: Disaster recovery plans and backup restore procedures must be tested semi-annually to ensure data can be successfully restored.

2.3 Disaster Recovery Policy

1. Disaster Recovery Plan (DRP): A documented disaster recovery plan must be developed and reviewed annually. The plan should include detailed recovery procedures for critical systems, communication protocols, and roles/responsibilities.
2. Recovery Time Objectives (RTO) & Recovery Point Objectives (RPO): Define RTO and RPO for each critical system to ensure systems can be recovered within the acceptable time and data loss limits.
3. Incident Response: In the event of a disaster, an incident response team must be activated to manage the recovery process.

3. User Setup and Termination Policy

3.1 Purpose

This policy governs the procedures for setting up new user accounts, modifying existing accounts, and terminating accounts to maintain security and data integrity.

3.2 User Setup

1. Authorization: All user accounts must be authorized by department heads and approved by IT management.
2. Access Control: Users should only be granted access to the systems and data necessary to perform their job functions (Principle of Least Privilege).

3. Account Creation: User accounts must be created with unique identifiers and strong, complex passwords. Two-factor authentication (2FA) is required for all accounts with access to critical systems.
4. Training: New users must complete IT security training before accessing the network and systems.

3.3 User Termination

1. Account Deactivation: Upon employee or contractor termination, user accounts must be deactivated immediately to prevent unauthorized access.
2. Access Revocation: Access to company networks, email, VPN, cloud services, and physical devices must be revoked within 24 hours of termination.
3. Data Handling: Data and files owned or managed by terminated users must be transferred to their supervisor or archived as required by the company's data retention policy.

4. Physical and Logical Security Policy

4.1 Purpose

This policy defines the requirements for protecting the company’s physical and digital assets from unauthorized access, tampering, or theft.

4.2 Physical Security

1. Access Control: Physical access to server rooms, data centers, and other sensitive areas must be restricted to authorized personnel only.
2. Surveillance: Security cameras must be installed at entry points of sensitive areas and monitored regularly.
3. Visitor Policy: Visitors to sensitive areas must be logged, and their access should be escorted by authorized personnel.
4. Device Security: All company laptops, workstations, and mobile devices must have encryption enabled and be physically secured when not in use (e.g., lockable cabinets or cable locks).

4.3 Logical Security

1. Authentication: Multi-factor authentication (MFA) must be implemented for all critical systems and services.
2. Password Management: Passwords must meet complexity requirements (minimum length, special characters, etc.), and users must change their passwords every 90 days.

3. Account Lockout: After a predefined number of failed login attempts, user accounts must be locked to prevent brute force attacks.
4. Encryption: Sensitive data, both in transit and at rest, must be encrypted using industry-standard encryption algorithms.

5. Cybersecurity Policy

5.1 Purpose

This policy aims to protect the company's digital infrastructure, networks, and data from cyber threats, including malware, phishing, and unauthorized access.

5.2 Threat Monitoring and Prevention

1. Firewall & Intrusion Detection: Firewalls, intrusion detection/prevention systems (IDS/IPS), and antivirus software must be deployed and updated regularly.
2. Patch Management: All systems, applications, and software must be patched promptly when security updates are available.
3. Malware Protection: Anti-malware software must be installed and updated on all company systems. Regular scans must be performed to detect and remove malware.

5.3 Incident Response

1. Incident Reporting: Any cybersecurity incidents (e.g., phishing attempts, suspicious activity) must be reported to the IT department immediately.
2. Incident Response Plan (IRP): The company must maintain a documented IRP, detailing steps for containing and mitigating incidents, investigating the root cause, and reporting breaches to appropriate authorities.
3. Forensics: After a cybersecurity incident, logs and other relevant data must be preserved for forensic analysis.

5.4 Employee Awareness and Training

1. Phishing Simulations: The IT department should conduct regular phishing simulations to raise awareness and test employee response.
2. Security Awareness: All employees must complete annual cybersecurity awareness training, covering topics such as password hygiene, social engineering, and safe internet practices.

5.5 Vendor Security

1. Third-Party Assessments: All vendors with access to company systems or data must undergo security assessments to ensure they meet company security standards.
2. Data Sharing: Vendors must comply with the company's data handling and security policies. Contracts must include data protection clauses.

6. Compliance and Enforcement

6.1 Audits and Compliance

1. Internal Audits: IT security policies and procedures will be reviewed and audited annually to ensure compliance with regulatory requirements and industry best practices.
2. External Audits: The company may also be subject to external audits, particularly in industries where data protection regulations (e.g., GDPR, HIPAA) are applicable.

6.2 Non-Compliance

1. Disciplinary Action: Non-compliance with this policy, whether accidental or intentional, may result in disciplinary action, up to and including termination of employment.
2. Legal Action: Any actions leading to data breaches or regulatory violations may result in legal consequences for the company and responsible individuals.

Last Review Date: [Insert Date]
Next Review Date: [Insert Date]

This IT Policy Manual serves as the foundation for maintaining a secure, resilient, and efficient technology environment. All employees are expected to comply with these policies to protect company assets and data.