Security Policy Review and Enhancement

1. Introduction

A robust security policy is the foundation of an organization's cybersecurity framework, providing guidelines for safeguarding sensitive data, ensuring regulatory compliance, and mitigating security threats. This document outlines key strategies for access control, data protection, incident response, business continuity, compliance monitoring, and third-party risk management.

Organizations face evolving cybersecurity threats, requiring continuous evaluation and improvement of security measures. A well-structured security policy not only protects assets but also builds stakeholder trust, minimizes operational risks, and enhances business resilience.

2. Access Control Policy

2.1 Objective

The access control policy regulates and restricts access to networks, systems, and sensitive data. It ensures that only authorized personnel have the necessary access while maintaining security and compliance.

2.2 Types of Access Control

- **Discretionary Access Control (DAC):** Data owners control access rights.
- **Mandatory Access Control (MAC):** Centralized authority grants access based on classification levels.
- **Role-Based Access Control (RBAC):** Access is assigned according to job roles.
- **Attribute-Based Access Control (ABAC):** Factors such as device type, location, and time dictate access permissions.

2.3 Scope

This policy applies to all employees, contractors, vendors, and any other individuals who have access to the organization's information assets. It covers all systems, applications, databases, and physical access to restricted areas.

2.4 Key Access Control Measures

- **User Identification & Authentication:** Implement Multi-Factor Authentication (MFA) for all users.

2.4.1 The Necessity of Applying for an MFA:

1. All critical systems and data resources of the organization are protected only by Multi-Factor Authentication (MFA).
2. MFA is applied only in connection with certain data authentication actions. A password is the first factor of MFA, but a second or third factor of authentication will also be required.
3. MFA is implemented individually for each user account. Each user must complete their own MFA configuration securely.

- **Access Reviews & Monitoring:** Regularly audit and update user privileges.
- **Session Controls:** Enforce automatic session timeouts for inactive users.
- **Access Revocation:** Immediately revoke access for terminated or departing employees.

2.5 Passwords Password Security Principles:

- **Password Length**: Passwords should be 8-12 characters long, but the longer the password, the safer it is.
- **Password Complexity**: Passwords should contain a mixture of letters (both lower case and upper case), numbers, and special characters.
- **Password Change**: Passwords are to be changed every 60-90 days by the users.
- **Unique Device**: Each account must have a unique password and username, and the tests must be retaken.

3. Data Protection Policy

3.1 Objective

The data protection policy ensures the confidentiality, integrity, and availability of company data. It mitigates risks associated with unauthorized access, data breaches, and cyber threats.

3.2 Scope

This policy applies to all employees, contractors, and third-party vendors who access, process, or store company data. It encompasses physical, administrative, and technical controls required for effective data security

3.3 Data Classification

- **Public Data:** Freely shareable information (e.g., company website content).
- **Internal Data:** Restricted to employees (e.g., internal communications).
- **Confidential Data:** Requires access controls (e.g., financial reports, employee records).
- **Highly Confidential Data:** Subject to encryption and stringent access restrictions (e.g., intellectual property, personal identifiable information).

3.4 Data Security Measures

- **Encryption:** Implement AES-256 encryption for sensitive data at rest and in transit.
- **Backup & Recovery:** Maintain redundant backups in secure locations.
- **Data Loss Prevention (DLP):** Deploy tools to monitor and prevent unauthorized data transfers.
- **Secure Storage:** Restrict access to sensitive files through role-based permissions.
- **Cloud Security**: Cloud services must comply with industry security standards, and data stored in the cloud must be encrypted.
- **Secure File Sharing**: Employees must use company-approved file-sharing platforms with encryption and access controls instead of personal or unauthorized storage solutions.
- **Physical Security**: Server rooms, data centers, and office spaces must have strict access controls, including badge-based entry systems and surveillance cameras, to prevent unauthorized physical access to sensitive data.

4. Incident Response Policy

4.1 Objective

A structured incident response plan ensures timely detection, containment, and recovery from security incidents, minimizing business disruption and reputational damage.

4.2 This policy applies to all employees, contractors and third-party service providers and any entity interacting with company data systems or networks. It covers all types of security incidents including but not limited to unauthorized access, malware infections data breaches denial-of-service attacks insider threats and policy violations.

4.3 Incident Classification

- **Low:** Minor incidents with minimal impact.
- **Medium:** Affects limited users or systems.
- **High:** Major security breach requiring urgent intervention.
- **Critical:** Severe attack with financial, legal, or operational consequences.

4.4 Incident Response Steps

1. **Identification:** Detect potential security threats through continuous monitoring.
2. **Containment:** Isolate affected systems to prevent further damage.
3. **Eradication:** Remove malware, unauthorized access, or security vulnerabilities.
4. **Recovery:** Restore systems and validate integrity before resuming operations.
5. **Post-Incident Analysis:** Conduct root cause analysis and implement preventive measures.

5. Business Continuity & Disaster Recovery

5.1 Objective

Ensure uninterrupted business operations during and after a security breach, cyberattack, or natural disaster.

5.2 Risk Sources

Natural disasters and man-made incidents can be equally damaging in different ways. Knowing the common sources of risks sets you up with a starting point to set up plans for handling them. Now that you've identified the key risk sources, you can move forward into crafting strategies to avoid the consequences of risks and develop mitigation strategies.

5.3 Key Strategies

- **Risk Assessment:** Identify threats such as cyberattacks, data loss, and infrastructure failures.
- **Redundant Systems:** Maintain offsite and cloud-based backups.
- **Disaster Recovery Testing:** Regularly test failover mechanisms and data restoration processes.
- **Alternative Communication Channels:** Establish emergency communication protocols.

5.4 Create a back-up

Creating a backup of your important data is crucial to ensure that you can recover it in case of loss or damage.It should be determined which data will be backed up.There are several ways to back up your data.

- **Cloud Backup**: Use cloud storage services like Google Drive, Dropbox, or OneDrive to store your data online. Cloud services are convenient and can be accessed from anywhere.
- **USB Flash Drive**: If you have a smaller amount of data, a USB flash drive can serve as a quick and portable backup solution.

6. Compliance & Security Monitoring

6.1 Objective

Ensure compliance with international regulations and industry standards while monitoring security events in real time.

6.2 Compliance Standards

- **ISO 27001:** Information Security Management System (ISMS) best practices.
- **GDPR:** Data privacy and protection requirements.
- **HIPAA:** Health data security for healthcare organizations.
- **NIST 800-53:** U.S. government security controls.

6.3 Security Monitoring Measures

- **SIEM Solutions:** Security Information and Event Management (SIEM) for real-time threat detection.
- **Regular Audits & Assessments:** Conduct security audits, penetration tests, and risk assessments.
- **Policy Enforcement:** Define disciplinary actions for policy violations.

7. Third-Party Risk Management

7.1 Objective

Ensure third-party service providers follow security best practices and do not introduce additional vulnerabilities to the organization.

7.2 Vendor Security Measures

- **Risk Assessments:** Evaluate security measures before engaging vendors.
- **Contractual Safeguards:** Include confidentiality agreements, SLAs, and compliance clauses.
- **Ongoing Security Reviews:** Regularly audit vendor security posture.
- **Incident Handling:** Ensure vendors have incident response procedures.
- **Termination Procedures:** Securely offboard vendors, ensuring data protection and regulatory compliance.

Conclusion

By implementing these security policies, organizations can enhance their cybersecurity posture, reduce risks, and ensure compliance with regulatory requirements. Continuous evaluation, monitoring, and improvement of security controls will help in adapting to emerging threats and maintaining business continuity.

A well-maintained security framework fosters trust among stakeholders, enhances resilience, and safeguards an organization's digital assets in an increasingly complex threat landscape.