Security Policies and Governance Report

1. Introduction

In this project, I aimed to create a cohesive security policy framework that aligns with best practices and regulatory requirements. By focusing on **Access Control**, **Data Protection**, and **System Use Policies**, I ensured that the foundational elements of my organization's security posture are addressed. I also established a governance structure to clarify roles and responsibilities, referenced a recognized security standard, and provided evidence of practical policy enforcement.

2. Policy Development Framework

I followed a structured approach to develop and refine my security policies:

1. **Requirements Gathering**

- I reviewed the organization's objectives, risk appetite, and relevant regulatory or industry standards (e.g., ISO 27001).

- I identified key stakeholders (IT teams, department heads, legal advisors) to understand their operational needs and constraints.

2. **Drafting and Review**

- I created draft versions of the policies for **Access Control**, **Data Protection**, and **System Use**.

- I circulated these drafts among stakeholders for feedback, ensuring alignment with business goals and compliance requirements.

3. **Approval and Publication**

- After incorporating stakeholder feedback, I finalized the policies and submitted them to the executive team (or designated authority) for formal approval.

- Once approved, I published the policies in a secure, easily accessible repository (e.g., an internal SharePoint site).

4. **Ongoing Maintenance**

- I scheduled periodic reviews (annually or after major organizational changes) to keep the policies current.

- I established a process for revisions and version control to track changes over time.

This framework helped me maintain clarity and consistency throughout the policy creation and management process.

3. Security Policy Document

3.1. Access Control Policy

Purpose:

To ensure that access to systems, applications, and data is granted based on the principle of least privilege and is properly authorized, authenticated, and audited.

Scope:

This policy applies to all employees, contractors, and third-party vendors who require access to the organization's information systems.

Key Requirements:

1. **User Account Management**

- **Provisioning**: Accounts must be created following a formal request and approval process.

- **Deprovisioning**: Accounts should be promptly disabled or removed upon termination of employment or contract.

- **Access Reviews**: Department heads must review user privileges at least quarterly to ensure appropriate access levels.

2. **Authentication**

- **Multi-Factor Authentication (MFA)**: All privileged and remote access must use MFA where possible.

- **Password Policy**: Passwords must be a minimum of 12 characters, include complexity (uppercase, lowercase, digits, special characters), and be changed regularly based on organizational guidelines.

3. **Authorization**

- **Least Privilege**: Access rights must be limited to the minimum necessary for users to perform their job duties.

- **Role-Based Access Control (RBAC)**: Roles must be defined for each department, and permissions assigned based on job function.

4. **Monitoring and Logging**

- **Audit Trails**: All access events (logins, privilege escalations) must be logged and retained for at least 90 days.

- **Alerting**: Suspicious login attempts or unauthorized access attempts must trigger alerts to the SOC team.

3.2. Data Protection Policy

Purpose:

To safeguard the confidentiality, integrity, and availability of sensitive data throughout its lifecycle, from creation or acquisition to storage, transmission, and eventual destruction.

Scope:

This policy covers all data classified as confidential or sensitive, as well as all employees and third parties who handle such data.

Key Requirements:

1. **Data Classification**

- **Categories**: Data must be classified into tiers (e.g., Public, Internal, Confidential, Highly Confidential).

- **Labeling**: All confidential or sensitive data must be clearly labeled, and employees must follow handling procedures based on classification.

2. **Data Handling**

- **Encryption**: Sensitive data must be encrypted at rest and in transit using industry-standard protocols (e.g., AES-256, TLS 1.2+).

- **Storage**: Confidential data must be stored on secure servers or encrypted cloud storage solutions approved by the IT department.

3. **Data Retention and Disposal**

- **Retention Schedule**: Retain data only as long as needed to meet business, legal, or regulatory requirements.

- **Secure Destruction**: When data is no longer required, it must be securely wiped or destroyed following approved methods (e.g., physical shredding, secure erase tools).

4. **Incident Response**

- **Data Breach Reporting**: Any suspected data breach involving sensitive information must be reported immediately to the Incident Response Team.

- **Containment and Recovery**: The Incident Response Plan outlines steps for containing data breaches and restoring affected systems.

3.3. System Use Policy

Purpose:

To define acceptable use of the organization’s information systems, networks, and equipment, ensuring productivity and security are maintained.

Scope:

All employees, contractors, and third parties using the organization’s systems, networks, or devices.

Key Requirements:

1. **Acceptable Use**

- **Business Purposes**: Company systems are to be used primarily for legitimate business activities.

- **Minimal Personal Use**: Reasonable personal use is allowed if it does not interfere with job responsibilities or security.

2. **Prohibited Activities**

- **Unauthorized Software**: Installation or use of unapproved software is strictly prohibited.

- **Malicious Behavior**: Users must not engage in activities that disrupt network operations, such as spreading malware or launching denial-of-service attacks.

3. **Remote Access**

- **VPN Requirement**: Users must use a secure VPN when accessing company systems from external networks.

- **Device Security**: Personal devices used for remote access must comply with company security standards (e.g., updated OS, antivirus installed).

4. **Monitoring**

- **Network Monitoring**: The organization reserves the right to monitor network traffic and system logs to detect unauthorized activities.

- **Privacy Expectations**: While the organization respects user privacy, no user should expect complete anonymity when using company resources.

4. Governance Structure

To enforce these policies effectively, I established a clear governance model:

1. **Executive Sponsor (CISO / CIO)**

- Provides overall direction and resources for implementing and maintaining security policies.

- Approves major policy updates and ensures alignment with organizational strategy.

2. **Policy Committee**

- Composed of representatives from IT, HR, Legal, and relevant business units.

- Reviews and updates policies on a scheduled basis or when significant changes occur.

- Resolves any conflicts or ambiguities in policy interpretation.

3. **Department Managers**

- Ensure their teams understand and comply with the policies.

- Identify and communicate unique departmental requirements or risks to the Policy Committee.

4. **IT Security Team / SOC**

- Monitors network activity, investigates potential policy violations, and enforces technical controls (e.g., firewalls, access controls).

- Provides regular reports to the Policy Committee on policy adherence and security incidents.

5. **Employees and Contractors**

- Responsible for reading and acknowledging the policies.

- Must report suspected violations or security incidents to the IT Security Team.

5. Compliance Requirements

I referenced **ISO/IEC 27001**—an internationally recognized information security management standard—to ensure that my policies align with best practices and compliance requirements. Specifically:

- **ISO 27001: A.9 Access Control**: My Access Control Policy aligns with the standard's emphasis on least privilege, user authentication, and regular access reviews.

- **ISO 27001: A.8 Asset Management**: The Data Protection Policy addresses asset classification, labeling, and secure disposal.

- **ISO 27001: A.7 Human Resource Security**: The System Use Policy includes guidelines for acceptable use, aligning with user responsibility requirements.

By mapping my policies to these ISO 27001 controls, I can demonstrate adherence to recognized security benchmarks and strengthen the organization's overall security posture.

6. Policy Implementation and Enforcement

6.1. Communication

1. **Policy Portal**: I published the approved policies on an internal SharePoint portal.

2. **Training Sessions**: I conducted mandatory security awareness sessions, highlighting the key points of each policy.

3. **Email Announcements**: I sent out organization-wide emails summarizing the new policies and linking to the full documents.

6.2. Enforcement Measures

1. **Technical Controls**:

- **Access Control**: Implemented role-based access control (RBAC) in Active Directory to enforce the Access Control Policy.

- **Encryption**: Enabled full-disk encryption on corporate laptops and required TLS for email communication to meet Data Protection requirements.

- **Monitoring**: Deployed network monitoring tools to detect unauthorized software installations or policy violations as stated in the System Use Policy.

2. **Acknowledgement**:

- All employees were required to sign a policy acknowledgement form during onboarding and after major policy updates.

- Non-compliance could result in disciplinary action, as outlined in the HR handbook.

3. **Reporting and Auditing**:

- **Regular Audits**: I scheduled quarterly audits to verify that technical controls are in place and that employees are adhering to the policies.

- **Incident Handling**: If an incident or policy violation occurs, the SOC team investigates, documents findings, and escalates to management if needed.

7. Conclusion

Through this project, I have developed a structured approach to **Security Policy and Governance** by:

1. **Creating a Policy Development Framework**: I followed a systematic process of drafting, reviewing, and approving security policies.

2. **Defining Key Security Policies**: I addressed **Access Control**, **Data Protection**, and **System Use** as foundational elements of an effective security program.

3. **Establishing a Governance Structure**: I outlined clear roles and responsibilities to enforce these policies.

4. **Referencing ISO 27001**: I mapped my policies to internationally recognized standards to ensure compliance and best practices.

5. **Implementing and Enforcing Policies**: I communicated the policies to all employees, deployed technical controls, and set up regular audits to maintain compliance.

By meeting these requirements, I demonstrated my ability to design, communicate, and enforce a robust security policy framework, ensuring that organizational assets and data are protected in alignment with business objectives and regulatory standards.

End of Report