Security Policy Review and Enhancement

A security policy is a document that outlines the rules and methods an organization uses to protect its data. It includes general security goals and covers specific issues like remote access, acceptable use and data collection. It is used with other documents, like standard operating procedures, to help achieve security goals.

Access Control Policy

1. Objective

- Access Control is a set of security measures used to control and restrict access to a user or system's resources. It is used to protect data, programs, and physical locations.
- This Access Control Policy establishes the principles, rules, and practices for how access to systems, data, and resources is granted, controlled, and monitored within the company. The policy ensures that only authorized users have the appropriate access to necessary information while maintaining security and compliance obligations. With adequate access control mechanisms, the company minimizes risks related to unauthorized access, data breaches, and insider threats.

1.1 Types of Access Control

The Four Types Of Access Control Are As Follows:

- **Discretionary Access Control (DAC):** Who is permitted access to a protected system, piece of data or resource depends on who owns or controls it in DAC.
- **Mandatory Access Control (MAC):** Users are given access under this non-discretionary model based on information clearance. Depending on the different degrees of security, a central authority controls access privileges. It is frequently employed in official and military contexts.
- **Role-based Access Control (RBAC):** RBAC allows access based on predetermined business functions rather than offering access based on a user's identification. Users should only have access to data that is necessary for doing their work within the company. This widely used strategy is built on roles, authorizations, and permissions.
- **Attribute-Based Access Control (ABAC):** With ABAC, access to both individuals and resources can be restricted based on a dynamic set of characteristics and environmental factors, such as the time of day and the location.

2. 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.

3. Access Control Policy

3.1 Access to networks and network services

- The network and network services that are necessary for the user's employment should be restricted to those who need access to them.
- Policy must address: networks and network services in scope for access; authorization procedures for indicating who (role-based) is permitted to access what and when; and management control to prevent or monitor access in the real world.

3.1.0 The company's network and network services include:

- Mail Servers
- Firewalls
- VPNs
- IDS/IPS systems
- Web Servers

3.2 User registration and management

- Creating New Users: When creating new users, rights should be assigned only according to their roles.
- User Rights Management: User rights can be used over time. In this case, they should be subject to defined changes and special controls should be considered.
- Closing and Deleting User Accounts: Accounts of terminated or changed customers should be closed or deleted.

3.3 User Access Provisioning

The process of user access provisioning should be designed to ensure that only authorized users are able to gain access to the system, and that they only have the level of access that is appropriate for their needs.

- Identification and authentication of users.
- Assignment of permissions and roles.
- Management of user accounts.
- Review of user access.
- 60 days after termination of user access.

3.4 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.

3.5 Authentication

Multi-factor authentication (MFA) is a backup method that uses three or more factors to verify a user's identity.

The Necessity of Applying for an MFA:

- All critical systems and data resources of the organization are protected only by Multi-Factor Authentication (MFA).
- 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.
- MFA is implemented individually for each user account. Each user must complete their own MFA configuration securely.

3.6 Removal of access rights

As we have also indicated, on termination of a contract of employment, agreement or arrangement (or, if appropriate, on variation by job change), extensive rights of access to information and data processing facilities should be terminated.

4. Review and Revision

Review Frequency: This policy will be reviewed at least annually to ensure its continued relevance and effectiveness. Reviews may also occur if there are significant changes in the organization's IT infrastructure or compliance requirements.

Revision Process: Any revisions to this policy will be carried out by the Information Security Team in coordination with relevant departments. Changes will be documented, and the updated policy will be communicated to all personnel.

Approval: All revisions to this policy must be approved by the Chief Information Security Officer (CISO) or designated authority.

Data Protection Policy

1. Objective

Data protection is about securing personal data from misuse, loss, or damage. This includes any data that can be associated with individuals or used to uniquely identify them, including Social Security number, driver’s license number, email address, gender, ethnicity, family members’ names, fingerprints, photos, healthcare data, political beliefs, and much more.This Data Security Policy outlines the measures and protocols to protect the company's data from unauthorized access, disclosure, alteration, and destruction.

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.

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.

The scope includes:

- All company-owned or managed IT infrastructure, including servers, endpoints, network devices, and cloud-based services.
- Data stored, transmitted, or processed on company systems, regardless of location.
- Remote work environments where employees access corporate data.
- Third-party service providers and partners handling company data.
- Security controls related to data access, authentication, and monitoring.
- Incident response and risk management practices to mitigate security threats.

3. Data Classification

Company data is classified into the following categories, ensuring appropriate protection measures are applied to each level:

- **Public:** Information that can be shared freely without risk to the company. Examples include marketing materials, job postings, and press releases.
- **Internal Use Only:** Data that is not meant for public disclosure but does not pose significant risks if exposed. Examples include internal memos, meeting notes, and company policies.
- **Confidential:** Sensitive business information requiring restricted access. Examples include customer information, employee records, internal financial reports, and operational plans. Access is limited to authorized personnel only.
- **Highly Confidential:** Critical data requiring the highest level of protection. Examples include trade secrets, intellectual property, legal documents, executive strategy documents, and personally identifiable information (PII). This data must be encrypted both in transit and at rest, with strict access controls and logging in place.

4. Data Protection Measures

To ensure the confidentiality, integrity, and availability of company data, the following protection measures will be implemented:

- **Encryption:** All sensitive data must be encrypted using industry-standard encryption algorithms (e.g., AES-256) in transit and at rest. Encryption keys must be securely stored and managed through a key management system (KMS).
- **Data Masking and Tokenization:** Where applicable, sensitive data must be masked or tokenized to limit exposure during processing and storage.
- **Secure Backup and Recovery:** Regular, encrypted backups must be taken and stored in multiple secure locations. Periodic testing of backup restoration processes will be conducted to ensure data availability in case of incidents.
- **Network Security:** Firewalls, intrusion detection and prevention systems (IDS/IPS), and secure VPNs must be used to protect data from unauthorized access and cyber threats.
- **Endpoint Security:** All company devices must have up-to-date security software, including antivirus, endpoint detection and response (EDR), and host-based intrusion prevention systems (HIPS).
- **Data Loss Prevention (DLP):** DLP solutions must be deployed to monitor, detect, and prevent unauthorized data exfiltration through email, cloud services, and external storage devices.
- **Access Logging and Monitoring:** Continuous monitoring solutions must be implemented to track access and modifications to sensitive data. Security Information and Event Management (SIEM) systems will be used for real-time threat detection.
- **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.
- **Secure Development Practices:** Applications handling sensitive data must follow secure coding practices (e.g., OWASP Top 10 guidelines) to prevent security vulnerabilities such as SQL injection and cross-site scripting (XSS).
- **Third-Party Risk Management:** Vendors handling company data must comply with security requirements, undergo security assessments, and sign data protection agreements (DPAs).
- **Mobile Device Management (MDM):** Company mobile devices must be protected through MDM solutions, enforcing security policies such as remote wiping and encryption.
- **Cloud Security:** Cloud services must comply with industry security standards, and data stored in the cloud must be encrypted. Security controls such as multi-factor authentication and access restrictions must be applied to cloud storage.
- **Patching and Vulnerability Management:** Regular updates and security patches must be applied to software, operating systems, and firmware to protect against known vulnerabilities.
- **Secure File Sharing:** Employees must use company-approved file-sharing platforms with encryption and access controls instead of personal or unauthorized storage solutions.

5. Employee Responsibilities

In the framework of data protection (Data Protection), the responsibilities of employees are of great importance, because the organization's information security is not only provided by technological solutions, but also relies on the human factor.

Data protection within an organization is not limited to strong encryption, firewalls and other technical security solutions. The role of people in this process is extremely important, as employees work with a variety of sensitive and confidential information in their daily activities. Even a small security

mistake made by an employee can lead to serious data leaks, financial losses, and even reputational incidents.

In addition, social engineering attacks, phishing, and malware (malware) take advantage of the employee distraction control systems used. For example, an employee may create security by opening an email brute-force and grant access to hackers. Therefore, enrollment in training for ongoing monitoring of collaboration, cyber threat awareness, and critical control measures is firmly defined in the organization's validation rules.

Employees must adhere to the following responsibilities:

- **Security Awareness & Training:** Employees must complete regular security awareness training, including phishing and social engineering awareness programs. Training sessions will be held periodically to keep employees informed about evolving threats and best practices.
- **Password Management:** Employees must create and maintain strong passwords that meet NIST password guidelines. Passwords must be unique, changed regularly, and never shared with unauthorized individuals.
- **Data Handling:** Employees must handle data according to its classification level. Confidential and Highly Confidential data must be accessed only when necessary and shared strictly on a need-to-know basis.
- **Device Security:** All company-provided and personal devices used for work purposes must have endpoint protection, including antivirus software and firewalls. Employees must ensure their devices are updated with the latest security patches.
- **Email & Communication Security:** Employees must be cautious when handling email attachments and links. They must verify the authenticity of any request involving sensitive data before responding or sharing information.
- **Remote Work Compliance:** Employees working remotely must use a company-approved VPN and avoid accessing company data from public or unsecured networks. They should ensure their work environment is secure and free from unauthorized access.
- **Reporting Security Incidents:** Any suspicious activity, phishing attempts, or security breaches must be reported immediately to the IT Security Team. Employees should not attempt to handle security incidents on their own.

6. Third-party security

Third-party risk management (TPRM) identifies, assesses and mitigates risks associated with outsourcing tasks to third-party vendors or service providers.

In an increasingly interconnected and outsourced world, third-party risk management (TPRM) is an essential business strategy. TPRM identifies and mitigates the risks that organizations face from engaging with external vendors or service providers. These third parties might be involved in various business functions, ranging from IT services and software development to supply chain management and customer support.

The need for TPRM arises from the inherent vulnerabilities associated with third-party relationships. Outsourcing tasks can bring benefits such as cost savings, scalability and access to specialized expertise, but it also exposes organizations to potential issues. TPRM aims to provide organizations with a comprehensive understanding of their third-party business relationships and the safeguards

that these vendors employ. This helps prevent problems such as operational disruptions, security breaches and compliance failures.

6.1 Third-party risk management lifecycle

An effective TPRM lifecycle helps organizations manage third-party risks and create secure, compliant and beneficial vendor relationships. Common TPRM lifecycle phases include:

6.1.0 Vendor discovery

Organizations identify third parties by consolidating existing vendor information, integrating with existing technologies and conducting assessments or interviews with internal business owners. This phase includes building an inventory of the third-party ecosystem and classifying third-party vendors based on the inherent risks they pose to the organization.

6.1.1 Vendor evaluation

Organizations review RFPs and select new vendors based on specific business needs and criteria. This involves assessing risk exposure and may require questionnaires and on-site evaluations to verify the accuracy and effectiveness of their internal security and information security measures. Key factors considered include the vendor's security ratings and posture, compliance with industry standards and overall fit with organizational requirements.

6.1.2 Risk analysis

Organizations conduct thorough risk assessments of selected vendors using various standards (for example, ISO 27001, NIST SP 800-53) to understand potential risks. Some use third-party risk exchanges to access pre-completed assessments, while others employ assessment automation software or spreadsheets.

6.1.3 Risk mitigation

After assessing the risks, organizations conduct risk mitigation. This involves flagging and scoring risks, determining if the risk levels are acceptable within the organization's risk appetite and implementing required controls to reduce risks to acceptable levels. Continuous monitoring is used to identify events that may alter the risk profile, such as data breaches or regulatory changes.

6.1.4 Contract negotiation and onboarding

This phase may overlap with risk mitigation and involves negotiating and finalizing contracts with vendors. Key aspects include making sure that contracts include critical provisions such as confidentiality clauses, NDAs, data protection agreements and service level agreements (SLAs). Contracts should be structured to address key risk management concerns and compliance requirements. Vendors are onboarded by integrating them into the organization’s systems and processes.

6.1.5 Documentation and reporting

Organizations maintain detailed records of all third-party interactions and risk management activities. Implementing TPRM software can facilitate comprehensive and auditable recordkeeping, enabling better reporting and compliance.

6.1.6 Continuous monitoring

Continuous monitoring of third-party vendors is crucial as it provides ongoing insights into their security posture and risk levels. Key events to monitor include regulatory changes, financial viability and any negative news that might affect the vendor's risk profile.

6.1.7 Vendor termination

When terminating vendor relationships, organizations must ensure that all data and assets are securely returned or disposed of and that detailed records of the offboarding process are maintained for compliance purposes. An offboarding checklist can help ensure that all necessary steps are taken.

7. Compliance and Monitoring

- **Regular Audits & Assessments:** The company will conduct regular security audits, penetration testing, and vulnerability assessments to ensure compliance with ISO 27001, NIST 800-53, and other regulatory standards.
- **Continuous Monitoring:** Security Information and Event Management (SIEM) solutions will be used to monitor network traffic, detect anomalies, and respond to potential threats in real-time.
- **Incident & Breach Reporting:** All security incidents must be documented and reviewed for compliance violations. Lessons learned will be used to enhance security policies.
- **Policy Enforcement:** Non-compliance with security policies will result in disciplinary actions, including access revocation, termination, or legal consequences, depending on severity.
- **Regulatory Compliance:** The organization will ensure alignment with applicable laws, regulations, and industry best practices, including GDPR, HIPAA, and PCI DSS where applicable.

8. Review and Revision

Review Frequency: This policy will be reviewed at least twice a year to ensure its continued relevance and effectiveness. Reviews may also occur if there are significant changes in the organization's IT infrastructure or compliance requirements.

Revision Process: Any revisions to this policy will be carried out by the Information Security Team in coordination with relevant departments. Changes will be documented, and the updated policy will be communicated to all personnel.

Approval: All revisions to this policy must be approved by the Chief Information Security Officer (CISO) or designated authority.

Incident Response Policy

1. Objective

This policy aims to ensure rapid detection and effective response to security incidents, minimize business disruption, protect sensitive data from unauthorized access or loss, enhance coordination among internal teams and external stakeholders, maintain regulatory compliance, and continuously improve security measures through periodic reviews and lessons learned.

2. Scope

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.

3. Incident Classification

Incident severity levels are critical for determining how quickly an organization should respond to a security incident. They are used to prioritize incidents and allocate resources for resolution. These levels often correspond to the potential impact on the organization, and typically range from low to critical.Security incidents are categorized based on severity and impact:

- Low (Minor Incident): No significant impact on operations.
- Medium (Moderate incident): Some impact on business functions but manageable.
- High (Major Incident): Significant disruption requiring immediate response.
- Critical (severe incident): Major compromise with financial, reputational or legal consequences.

4. Incident management

4.1 Create an incident management strategy

Your company should have a written policy detailing the goals, boundaries, and accountability for incident management.

4.2 Establish incident management procedures

Establish thorough protocols that spell out how occurrences will be located, evaluated, dealt with, reported, analyzed, and reviewed. These protocols describe the roles and duties of individuals or teams participating in incident management, as well as the routes for communication and escalation procedures.

4.3 Identification and recording of incidents

Implement systems for quickly detecting and documenting security incidents. Utilizing different monitoring tools, automated warnings, intrusion detection systems, or staff reporting channels may be necessary for this. Make sure to record the crucial details about occurrences, such as the date, time, incident's nature, impact, and a preliminary assessment.

4.4 Response to incidents and containment

Create an organized and precise incident response procedure. Define the procedures you will follow in response to various incidents, such as early evaluation, containment of the incident to stop additional harm, and restoration of impacted systems or data. Assign individuals or teams involved in the event response with clear roles and duties.

4.5 Reporting of incidents

Create a system for tracking and reporting events. This entails compiling incident reports that contain comprehensive details regarding the incident, the responses made, and any subsequent steps needed. Moreover, reports on incidents are important sources of information for analysis, spotting trends, and making adjustments in the future.

4.6 Analysis and investigation of incidents

Investigate incidents thoroughly to ascertain their underlying causes, effects, and scope. Also, examine the underlying deficiencies or vulnerabilities that caused the incident to happen. This research aids in locating areas where security controls, procedures, and staff awareness should be strengthened. Apply corrective measures in light of the findings to stop such occurrences in the future.

5. Disaster recovery plan

Disaster recovery plan specifies the actions you can take if an incident impacts your company's information security systems.Disaster recovery plan implements several measures to ensure all data is backed up regularly and securely.

With the right technology solutions in place – cloud computing, quick data recovery, and encryption, you can mitigate the impact of an information security incident by deploying quick restoring protocols. Making sure the plan is effective in restoring IT services within a negotiated timeframe is key; it's like an insurance policy for business continuity.

5.1 Establish a Business Continuity Management System

Establishing a business continuity management system (BCMS) is a critical first step in developing a disaster recovery plan. A BCMS equips businesses with the policies, procedures, and processes needed to recover efficiently from disruption. This comprehensive system can be tailored to the company's specific needs and objectives.

5.2 Identify 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.

Some disasters may include:

- Fires
- Cyberattacks
- Information leakage
- Change of trend
- Power outages
- Failure in plans

5.3 Develop Mitigation Strategies

Developing mitigation strategies is essential to reducing the damages of unexpected disruptions. For example, having a backup generator to keep computers running and communications networks connected during a power outage can be invaluable.

Offsite data storage means that vital data won't be lost when an office is closed or destroyed. Having redundant communication systems in place provides continuity in times of crisis.

5.4 Create a back-up of your important data

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. Choose the method that suits you best:

- **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.
- **External Hard Drive**: Use an external hard drive or SSD to create a physical backup. This is a good option if you have large files or prefer offline storage.
- **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. Review and Revision

Review Frequency: This policy will be reviewed at least twice a year to ensure its continued relevance and effectiveness. Reviews may also occur if there are significant changes in the organization's IT

infrastructure or compliance requirements.

Revision Process: Any revisions to this policy will be carried out by the Information Security Team in coordination with relevant departments. Changes will be documented, and the updated policy will be communicated to all personnel.

Approval: All revisions to this policy must be approved by the Chief Information Security Officer (CISO) or designated authority.

Note: All policies and procedures you see above have been developed in accordance with ISO/IEC 27001 and NIST CSF standards.