Heimdal®

Endpoint Security Policy Template

Purpose

The purpose of this policy is to define the standards, procedures, and requirements for protecting and managing the security of endpoint devices that connect to the organization's network or handle its data.

This includes, but is not limited to, desktop computers, laptops, tablets, mobile phones, and other devices that connect to the internal network or access company resources remotely.

Scope

This policy applies to all employees, contractors, consultants, temporaries, and other workers, including all personnel affiliated with third parties who use company-owned or personally owned endpoint devices to connect to the organization's network.

---

1. Definitions

- **Endpoint Device**: Any device that connects to the corporate network, such as desktops, laptops, smartphones, tablets, or any other device.
- **Malware**: Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems.
- **BYOD**: Bring Your Own Device, referring to personal devices used by employees to access the organization's resources.

---

2. Policy Statement

All endpoint devices must adhere to the organization's security standards and procedures to ensure they do not compromise the security, confidentiality, and integrity of organizational data.

This policy aims to reduce the risk of malware, data breaches, and unauthorized access by ensuring endpoint devices are secure and comply with the company's security requirements.

---

3. Responsibilities

- **IT Department**: Responsible for implementing, monitoring, and maintaining endpoint security tools, managing endpoint devices, and ensuring compliance.
- **Users**: Responsible for adhering to the security practices outlined in this policy, reporting suspicious activities, and maintaining the security of their assigned devices.
- **Management**: Ensure their teams comply with this policy and support enforcement actions if necessary.

---

4. Endpoint Security Controls

4.1 Device Registration and Inventory

- All endpoint devices must be registered with the IT department before being allowed to connect to the corporate network.
- IT must maintain an inventory of all devices accessing the network.

4.2 Encryption

- All data stored on endpoint devices must be encrypted using strong encryption standards (e.g., AES-256).
- Removable media (USB drives, external hard drives, etc.) must be encrypted if they contain sensitive data.

4.3 Authentication

- Multi-factor authentication (MFA) must be enabled on all endpoint devices that access the corporate network or sensitive data.
- Device passwords must meet the organization's complexity requirements (e.g., at least 8 characters, with a combination of upper and lower case letters, numbers, and special characters).
- Passwords must be changed at regular intervals (every 90 days).

4.4 Antivirus and Anti-Malware

- All endpoint devices must have up-to-date antivirus and anti-malware software installed and configured.
- Devices should perform regular scans for malware at least once a week.
- Any detected threats must be immediately reported to the IT department.

4.5 Patching and Updates

- All endpoint devices must be regularly patched and updated with the latest security updates, including both the operating system and applications.
- Automatic updates must be enabled on all endpoint devices.

4.6 Firewalls

- Devices must have host-based firewalls enabled and configured to block unauthorized access.
- Exceptions should only be made with approval from IT.

4.7 Device Locking

- Endpoint devices must lock automatically after a defined period of inactivity (no more than 15 minutes).
- Users should lock their devices when leaving them unattended.

---

5. Remote Access

- Remote access to corporate resources is only permitted through approved secure methods such as VPN, SSH, or secure cloud solutions.
- All remote connections must be encrypted using industry-standard protocols (e.g., IPsec, SSL).
- Only authorized personnel may connect to the company network remotely.

---

6. Bring Your Own Device (BYOD)

- Employees must request approval from IT before using personal devices for work purposes.
- All BYOD devices must comply with the same security standards as company-owned devices, including encryption, antivirus, and firewall settings.
- IT reserves the right to manage and remotely wipe corporate data from personal devices in the event of loss, theft, or when employment ends.

---

7. Incident Reporting

- All users must immediately report any suspected or confirmed security incidents related to endpoint devices to the IT department.
- Examples of incidents include device theft, loss of data, or detection of malware.
- Users must cooperate with the IT department in investigating and resolving incidents.

---

8. Data Backup

- Endpoint devices must regularly back up critical business data in line with the organization's backup policy.
- Data backups must be encrypted and stored in a secure location.

---

9. Monitoring and Auditing

- The organization reserves the right to monitor endpoint devices for compliance with security policies.
- Regular audits of endpoint security practices will be conducted to ensure compliance.

---

10. Enforcement

- Violations of this policy may result in disciplinary actions, including but not limited to the termination of employment or access privileges.
- Non-compliance with endpoint security requirements may result in a denial of access to the corporate network.

---

11. Exceptions

- Exceptions to this policy may only be granted by the IT department in conjunction with senior management and must be documented.

---

12. Policy Review

- This policy will be reviewed at least annually or whenever significant changes occur to ensure it remains up to date with the organization’s security requirements and industry best practices.

Approval

This policy has been reviewed and approved by the organization's executive team.

Company Name: [Insert Company Name]

Policy Contact: [Insert Contact Name or Department]

Effective Date: [Insert Date]

Review Date: [Insert Date]

Version: [Insert Version Number]