iGUIDE

ISMS

Information Security User Endpoint Devices

iNFOSECBASE

Contents

A Guide to Information Security User Endpoint Devices 3
Introduction 3
Objectives 3
Key Security Requirements for Endpoint Devices 3
Asset Management and Inventory Control 3
Access Control and Authentication 3
Protection Against Malware and Threats 3
Secure Configuration and Hardening 4
Secure Use of Cloud Services and Remote Access 4
Data Protection and Encryption 4
Physical Security of Devices 4
Secure Disposal and Reuse of Endpoint Devices 4
Best Practices for Implementing User Endpoint Devices Security Controls 4
Implementation Steps for User Endpoint Devices 5
Identify and Classify Endpoint Devices 5
Implement Access Controls and Authentication 5
Deploy Endpoint Security Solutions 5
Secure Remote Work and Cloud Access 5
Implement Data Encryption and Backup Strategies 5
Enforce Physical Security and Device Management 5
Establish a Secure Device Disposal Process 5
Summary 5

A Guide to Information Security User Endpoint Devices

Introduction

Endpoint devices are common targets for cyber threats, including malware, phishing and unauthorised access. Implementing strong security controls for these devices is essential to ensuring compliance with ISO 27001 and safeguarding critical business information.

Annex A.8.1 – User Endpoint Devices focuses on securing endpoint devices such as laptops, desktops, tablets and mobile phones. These devices are essential for business operations but also represent significant security risks if not properly managed. Organisations must implement security controls to ensure endpoint devices are protected against threats such as malware, unauthorised access, data loss and physical theft.

This guide covers the key controls, best practices and implementation steps for securing user endpoint devices in alignment with ISO 27001:2022.

Objectives

- To protect sensitive organisational data accessed or stored on endpoint devices.
- To minimise security risks arising from unauthorised access, malware infections and data breaches.
- To ensure endpoint devices are securely configured, maintained and monitored throughout their lifecycle.
- To enforce policies for secure usage, storage and disposal of endpoint devices.

Key Security Requirements for Endpoint Devices

Asset Management and Inventory Control

- Maintain an up-to-date inventory of all endpoint devices.
- Assign ownership and accountability for each device.
- Classify devices based on the sensitivity of the data they handle.

Access Control and Authentication

- Enforce strong authentication mechanisms such as passwords and multi-factor authentication (MFA).
- Implement role-based access control (RBAC) to restrict user privileges.
- Automatically lock devices after a period of inactivity.

Protection Against Malware and Threats

- Deploy endpoint protection tools, including antivirus, anti-malware and endpoint detection and response (EDR) solutions.
- Ensure automatic security updates and patches for operating systems and software.

- Restrict the installation of unauthorised applications.

Secure Configuration and Hardening

- Apply security baselines for device configurations.
- Disable unnecessary services, ports and applications.
- Encrypt data stored on endpoint devices and ensure secure data transmission.

Secure Use of Cloud Services and Remote Access

- Use Virtual Private Networks (VPNs) or Zero Trust Network Access (ZTNA) for secure remote connections.
- Implement policies for Bring Your Own Device (BYOD) usage.
- Monitor remote access logs for anomalies and security breaches.

Data Protection and Encryption

- Encrypt sensitive data on endpoint devices, both at rest and in transit.
- Implement data loss prevention (DLP) tools to prevent unauthorised data transfers.
- Regularly back up data stored on endpoint devices.

Physical Security of Devices

- Require employees to store endpoint devices securely when not in use.
- Use cable locks or physical security measures for devices in high-risk areas.
- Implement tracking mechanisms for corporate-owned devices.

Secure Disposal and Reuse of Endpoint Devices

- Ensure data is securely erased before reusing or disposing of devices.
- Follow approved methods such as cryptographic erasure or physical destruction of storage media.
- Maintain a log of decommissioned and disposed endpoint devices.

Best Practices for Implementing User Endpoint Devices Security Controls

- Develop and enforce an endpoint security policy that defines acceptable use, security requirements and compliance expectations for employees.
- Use Mobile Device Management (MDM) solutions to enforce security settings, remotely wipe lost or stolen devices and manage device compliance.
- Conduct regular security awareness training for employees on endpoint security risks such as phishing, social engineering and malware threats.
- Monitor endpoint devices for suspicious activities using endpoint security analytics and Security Information and Event Management (SIEM) tools.
- Regularly update security controls to address emerging threats and vulnerabilities in endpoint devices.

Implementation Steps for User Endpoint Devices

Identify and Classify Endpoint Devices

- Maintain an inventory of all endpoint devices used within the organisation.
- Classify devices based on data sensitivity and risk level.

Implement Access Controls and Authentication

- Enforce strong password policies and MFA.
- Restrict access based on user roles and job responsibilities.

Deploy Endpoint Security Solutions

- Install and configure antivirus, anti-malware and intrusion prevention software.
- Enable automatic updates for security patches.

Secure Remote Work and Cloud Access

- Require VPNs or Zero Trust solutions for remote access.
- Enforce encryption and secure cloud storage policies.

Implement Data Encryption and Backup Strategies

- Encrypt sensitive data stored on endpoint devices.
- Ensure regular backups to prevent data loss.

Enforce Physical Security and Device Management

- Require employees to store devices securely when not in use.
- Implement tracking mechanisms for company-owned devices.

Establish a Secure Device Disposal Process

- Use approved data erasure methods before disposing of devices.
- Maintain records of decommissioned endpoint devices.

Summary

User Endpoint Devices security focuses on securing endpoint devices to prevent unauthorised access, data breaches and security threats. Organisations must implement robust security measures, including:

- Maintaining an up-to-date inventory of endpoint devices.
- Enforcing access control and authentication measures.
- Deploying endpoint protection tools and ensuring timely updates.
- Securing remote access and implementing data encryption.
- Enforcing physical security measures for endpoint devices.
- Securely disposing of devices to prevent data leakage.

By integrating these controls into their ISMS, organisations can enhance endpoint security, protect sensitive data and comply with ISO 27001:2022 requirements.