Endpoint Security Policy Template

Document Control Information

- **Document Title:** Endpoint Security Policy
- **Document Version:** 1.0
- **Last Updated:** [DATE]
- **Document Owner:** [ROLE/NAME]
- **Approved By:** [ROLE/NAME]
- **Next Review Date:** [DATE]

1. Introduction

1.1 Purpose

This Endpoint Security Policy establishes [ORGANIZATION NAME]'s requirements for securing endpoint devices that access organizational information and systems in accordance with ISO 27001:2022 requirements. It provides a framework for protecting endpoints from security threats and ensuring they are configured, maintained, and operated securely.

1.2 Scope

This policy applies to: - All endpoint devices owned, leased, or managed by [ORGANIZATION NAME] - All endpoint devices used to access organizational information or systems - All types of endpoints, including: - Desktop computers - Laptop computers - Tablets and smartphones - Virtual desktops - Servers (physical and virtual) - Specialized devices and IoT devices - All employees, contractors, consultants, and third parties who use these devices - All environments, including corporate offices, remote locations, and home offices

1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Implementing appropriate security controls on all endpoint devices - Protecting endpoints from malware and other security threats - Ensuring endpoints are properly configured and maintained - Monitoring endpoints for security events and vulnerabilities - Responding effectively to endpoint security incidents - Providing users with guidance on secure endpoint usage - Continuously improving endpoint security controls

2. Endpoint Protection

2.1 Malware Protection

- All endpoints shall have approved anti-malware software installed
- Anti-malware software shall:
  - Be centrally managed where possible
  - Perform real-time scanning
  - Conduct scheduled full-system scans
  - Update signatures automatically
  - Be configured to prevent disabling by users
- Anti-malware alerts shall be monitored and addressed
- Anti-malware effectiveness shall be regularly assessed
- Additional protection layers shall be implemented where appropriate

2.2 Host Firewall

- Host-based firewalls shall be enabled on all endpoints
- Firewall configurations shall:
  - Block unauthorized inbound connections
  - Control outbound connections
  - Be centrally managed where possible
  - Follow least-privilege principles
- Firewall rules shall be documented
- Firewall configurations shall be regularly reviewed
- Firewall logs shall be monitored for security events

2.3 Intrusion Prevention

- Host-based intrusion prevention systems (HIPS) shall be implemented where appropriate
- HIPS shall be configured to:
  - Detect and block suspicious activities
  - Protect against exploitation attempts
  - Monitor system integrity
  - Alert on significant security events
- HIPS configurations shall be regularly reviewed
- HIPS effectiveness shall be regularly assessed
- HIPS alerts shall be monitored and addressed

2.4 Application Control

- Application control measures shall be implemented where appropriate

- Application control shall:
  - Allow only authorized applications to run
  - Block known malicious applications
  - Control application privileges
  - Be centrally managed where possible
- Application whitelisting shall be considered for high-security environments
- Application control exceptions shall be documented and approved
- Application control effectiveness shall be regularly assessed

3. Endpoint Configuration and Hardening

3.1 Secure Configuration

- Endpoints shall be configured according to security baselines
- Security baselines shall address:
  - Operating system security settings
  - Application security settings
  - Service configurations
  - Security features enablement
  - Default account management
- Baselines shall be documented and version-controlled
- Baseline compliance shall be regularly verified
- Deviations from baselines shall be documented and approved

3.2 System Hardening

- Endpoints shall be hardened to reduce attack surface
- Hardening shall include:
  - Removing or disabling unnecessary services
  - Removing or disabling unnecessary applications
  - Removing or disabling unnecessary user accounts
  - Restricting administrative privileges
  - Configuring security features
- Hardening procedures shall be documented
- Hardening effectiveness shall be regularly assessed
- Hardening shall be performed before deployment

3.3 Default Settings and Accounts

- Default settings shall be reviewed and secured
- Default accounts shall be:
  - Renamed where possible
  - Secured with strong passwords

    - Disabled if not required
- Default passwords shall be changed before deployment
- Default services shall be disabled if not required
- Default sharing shall be disabled if not required
- Default security features shall be enabled

3.4 Secure Boot and BIOS/UEFI

- BIOS/UEFI shall be password protected
- Secure Boot shall be enabled where supported
- Boot order shall be configured to prevent unauthorized booting
- BIOS/UEFI shall be kept updated
- BIOS/UEFI security features shall be enabled
- BIOS/UEFI configurations shall be documented
- Physical access to device internals shall be controlled

4. Authentication and Access Control

4.1 User Authentication

- Strong authentication shall be required for endpoint access
- Authentication shall include:
    - Complex passwords or passphrases
    - Multi-factor authentication where appropriate
    - Biometric authentication where appropriate
- Authentication failures shall be limited and logged
- Authentication credentials shall be protected
- Default credentials shall be changed
- Authentication methods shall be regularly reviewed

4.2 Privileged Access

- Administrative privileges shall be strictly controlled
- Privileged accounts shall:
    - Be provided only when required
    - Be used only for administrative tasks
    - Require stronger authentication
    - Be regularly reviewed
- Standard users shall not have administrative rights
- Privilege elevation shall be controlled and logged
- Privileged activities shall be monitored

4.3 Session Security

- Inactive sessions shall automatically lock after [15] minutes
- Session lock shall require authentication to unlock
- Users shall lock sessions when leaving devices unattended
- Multiple concurrent sessions shall be controlled
- Remote sessions shall have additional security controls
- Session security shall be enforced technically where possible
- Session security awareness shall be promoted

4.4 Physical Access Control

- Physical access to endpoints shall be controlled
- Unattended endpoints shall be physically secured
- Screen privacy filters shall be used in public areas
- Physical security measures shall be appropriate to location risk
- Physical security incidents shall be reported
- Physical security awareness shall be promoted
- Physical security shall be regularly assessed

5. Patch and Vulnerability Management

5.1 Patch Management

- Security patches shall be applied in a timely manner
- Critical patches shall be applied within [TIMEFRAME]
- Patch deployment shall be centrally managed where possible
- Patch compliance shall be monitored
- Patch exceptions shall be documented and approved
- Patch testing shall be performed before deployment
- Patch deployment shall follow change management procedures

5.2 Vulnerability Management

- Endpoints shall be regularly scanned for vulnerabilities
- Vulnerability assessments shall be performed:
  - After significant changes
  - After security incidents
  - At regular intervals
- Vulnerabilities shall be prioritized based on risk
- Remediation plans shall be developed for identified vulnerabilities
- Remediation progress shall be tracked
- Vulnerability trends shall be analyzed

- Vulnerability management effectiveness shall be assessed

5.3 End-of-Life Systems

- End-of-life systems shall be identified and documented
- Migration plans shall be developed for end-of-life systems
- Additional security controls shall be implemented for end-of-life systems
- End-of-life systems shall be isolated where possible
- End-of-life systems shall be replaced as soon as feasible
- Exceptions shall be documented and approved
- Risks associated with end-of-life systems shall be regularly assessed

6. Data Protection

6.1 Disk Encryption

- Full disk encryption shall be implemented on:
  - Laptops and portable devices
  - Desktops containing sensitive information
  - Removable media containing sensitive information
- Encryption shall use approved algorithms and key lengths
- Encryption keys shall be securely managed
- Recovery mechanisms shall be established
- Encryption implementation shall be verified
- Encryption exceptions shall be documented and approved
- Encryption effectiveness shall be regularly assessed

6.2 Data Loss Prevention

- Data loss prevention controls shall be implemented where appropriate
- Controls shall address:
  - Unauthorized data transfers
  - Unauthorized external storage use
  - Unauthorized cloud storage use
  - Unauthorized printing
  - Unauthorized screen capture
- DLP policies shall be based on data classification
- DLP alerts shall be monitored and addressed
- DLP effectiveness shall be regularly assessed

6.3 Removable Media Control

- Removable media usage shall be controlled

- Controls may include:
  - Technical restrictions on media use
  - Encryption requirements for media
  - Scanning media for malware
  - Logging media usage
  - Approval requirements for media use
- Unauthorized media shall be blocked where possible
- Authorized media shall be inventoried where appropriate
- Media handling procedures shall be documented

6.4 Information Handling

- Information handling procedures shall be established
- Procedures shall address:
  - Storing information on endpoints
  - Transferring information between endpoints
  - Printing sensitive information
  - Disposing of information
- Information handling shall align with classification requirements
- Information handling compliance shall be monitored
- Information handling awareness shall be promoted

7. Endpoint Monitoring and Logging

7.1 Security Monitoring

- Endpoints shall be monitored for security events
- Monitoring shall include:
  - Authentication events
  - Policy changes
  - System changes
  - Security control changes
  - Application installation/removal
  - Privilege use
- Monitoring shall be centralized where possible
- Monitoring data shall be protected
- Monitoring coverage shall be regularly assessed

7.2 Logging and Auditing

- Security-relevant events shall be logged
- Logs shall include:
  - Date and time

    - User identification
    - Activity description
    - Success or failure indication
    - Origin of event
- Logs shall be protected from tampering
- Logs shall be retained according to requirements
- Log review procedures shall be established
- Log storage capacity shall be monitored

7.3 Behavioral Monitoring

- Endpoint behavior shall be monitored where appropriate
- Behavioral monitoring shall detect:
    - Unusual user behavior
    - Unusual system behavior
    - Potential compromise indicators
    - Data exfiltration attempts
- Behavioral baselines shall be established
- Behavioral alerts shall be investigated
- False positives shall be tuned
- Behavioral monitoring effectiveness shall be assessed

8. Remote and Mobile Endpoints

8.1 Remote Endpoint Security

- Remote endpoints shall meet the same security requirements as on-premises endpoints
- Additional controls for remote endpoints may include:
    - VPN requirement for network access
    - Enhanced authentication
    - Increased monitoring
    - Stricter access controls
    - Regular compliance verification
- Remote endpoint security shall be regularly assessed
- Remote endpoint security awareness shall be promoted
- Remote endpoint security incidents shall be promptly addressed

8.2 Mobile Device Security

- Mobile devices shall be secured according to the Mobile Device Policy
- Mobile device security shall include:
    - Device encryption

    - Strong authentication
    - Remote wipe capability
    - Application controls
    - Configuration management
- Mobile device management (MDM) shall be implemented
- Mobile device compliance shall be monitored
- Lost or stolen devices shall be reported immediately

8.3 Bring Your Own Device (BYOD)

- BYOD usage shall be governed by a BYOD Policy
- BYOD security requirements shall include:
    - Minimum security controls
    - Acceptable use requirements
    - Support limitations
    - Privacy considerations
    - Organizational rights
- BYOD users shall agree to terms and conditions
- BYOD compliance shall be verified
- BYOD security shall be regularly assessed
- BYOD security incidents shall be promptly addressed

9. Endpoint Lifecycle Management

9.1 Procurement and Deployment

- Security requirements shall be defined before procurement
- New endpoints shall be securely configured before deployment
- Standard images shall be used where appropriate
- Images shall be regularly updated and secured
- Deployment procedures shall be documented
- Deployment shall include security verification
- Deployment exceptions shall be documented and approved

9.2 Maintenance and Support

- Endpoints shall be regularly maintained
- Maintenance shall include:
    - Operating system updates
    - Application updates
    - Security configuration verification
    - Performance optimization
    - Hardware maintenance

- Maintenance procedures shall be documented
- Maintenance shall be logged
- Maintenance effectiveness shall be assessed

9.3 Disposal and Reuse

- Endpoints shall be securely disposed of or reused
- Disposal procedures shall include:
    - Data sanitization
    - Software license management
    - Hardware recycling or destruction
    - Documentation updates
- Reuse procedures shall include:
    - Data sanitization
    - Reconfiguration
    - Security verification
- Disposal and reuse shall be documented
- Disposal and reuse effectiveness shall be verified

10. Incident Response

10.1 Endpoint Security Incidents

- Endpoint security incidents shall be promptly identified
- Incidents may include:
    - Malware infections
    - Unauthorized access
    - Data breaches
    - Policy violations
    - Physical theft or loss
- Incident response procedures shall be documented
- Incidents shall be reported according to procedures
- Incidents shall be investigated and remediated
- Incident lessons learned shall be incorporated into controls

10.2 Endpoint Isolation

- Compromised endpoints shall be isolated
- Isolation procedures shall be documented
- Isolation may be:
    - Network isolation
    - Physical isolation
    - Logical isolation

- Isolation shall be prompt and effective
- Isolation shall be maintained until remediation is complete
- Isolation effectiveness shall be verified
- Return to service shall follow verification procedures

10.3 Endpoint Recovery

- Compromised endpoints shall be recovered securely
- Recovery procedures shall be documented
- Recovery may include:
  - Reimaging
  - Restoration from backup
  - Reconfiguration
  - Verification
- Recovery shall address root causes
- Recovery shall be verified before return to service
- Recovery lessons learned shall be documented
- Recovery procedures shall be regularly tested

11. User Awareness and Training

11.1 Security Awareness

- Users shall receive endpoint security awareness training
- Awareness shall cover:
  - Security threats and risks
  - Security policies and procedures
  - User responsibilities
  - Incident reporting
  - Best practices
- Awareness shall be provided at onboarding and regularly thereafter
- Awareness effectiveness shall be measured
- Awareness materials shall be regularly updated

11.2 Technical Training

- Technical staff shall receive specialized endpoint security training
- Training shall cover:
  - Endpoint security technologies
  - Security configuration
  - Threat detection and response
  - Security assessment
  - Security tools and techniques

- Training shall be appropriate to job responsibilities
- Training shall be updated as technologies evolve
- Training effectiveness shall be assessed

12. Compliance and Exceptions

12.1 Compliance Monitoring

- Endpoint compliance shall be regularly monitored
- Monitoring shall include:
  - Security configuration compliance
  - Patch compliance
  - Software compliance
  - Policy compliance
- Non-compliant endpoints shall be identified and remediated
- Compliance reports shall be provided to management
- Compliance trends shall be analyzed
- Compliance monitoring effectiveness shall be assessed

12.2 Exceptions

Exceptions to this policy shall be: - Documented with justification - Risk-assessed and approved by the Information Security Manager - Time-limited and regularly reviewed - Accompanied by compensating controls where appropriate

13. Roles and Responsibilities

13.1 IT Department

- Implement and maintain endpoint security controls
- Deploy and manage endpoint security technologies
- Monitor endpoint security status
- Respond to endpoint security incidents
- Maintain endpoint security documentation
- Provide technical support for endpoint security
- Report on endpoint security status

13.2 Information Security Team

- Define endpoint security requirements
- Develop endpoint security policies and procedures
- Assess endpoint security effectiveness
- Investigate security incidents

- Provide security guidance and expertise
- Monitor emerging threats and vulnerabilities
- Report on security status to management

13.3 Department Managers

- Ensure staff compliance with endpoint security policies
- Report endpoint security issues
- Support endpoint security initiatives
- Include security in departmental processes
- Provide feedback on security controls
- Reinforce security awareness
- Support security incident response

13.4 All Users

- Comply with endpoint security policies
- Use endpoints securely
- Report security incidents and concerns
- Participate in security awareness training
- Maintain physical security of endpoints
- Follow secure information handling procedures
- Support security assessments and audits

14. Related Documents

- Information Security Policy
- Access Control Policy
- Mobile Device Policy
- Patch Management Policy
- Incident Response Policy
- Acceptable Use Policy
- [LIST OTHER RELEVANT POLICIES AND PROCEDURES]

15. Approval

This Endpoint Security Policy is approved by:

Name: _____ Position: _____ Date: _____ Signature: _____