Asset Management Policy Template

Document Control Information

- **Document Title:** Asset Management 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 Asset Management Policy establishes [ORGANIZATION NAME]'s requirements for identifying, classifying, managing, and protecting information assets throughout their lifecycle in accordance with ISO 27001:2022 requirements. It provides a framework for ensuring that assets are properly inventoried, owned, protected, and handled according to their value and sensitivity.

1.2 Scope

This policy applies to: - All information assets owned, leased, or managed by [ORGANIZATION NAME] - All physical assets that store, process, or transmit information - All software assets used within the organization - All employees, contractors, consultants, and third parties who use or have access to organizational assets - All locations where organizational assets are stored or used

1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Identifying and maintaining an inventory of all information assets - Assigning ownership and responsibility for all assets - Classifying assets according to their value, sensitivity, and criticality - Implementing appropriate protection for assets based on their classification - Managing assets throughout their lifecycle from acquisition to disposal - Ensuring the secure handling, storage, and disposal of assets - Complying with relevant legal, regulatory, and contractual requirements

2. Asset Identification and Inventory

2.1 Asset Identification

- All assets shall be identified and documented
- Assets shall be assigned a unique identifier
- Asset identification shall include:
  - Asset type
  - Asset description
  - Asset location
  - Asset owner
  - Asset custodian
  - Asset value
  - Asset classification
- Asset identification shall be performed during asset acquisition

2.2 Asset Inventory

- A comprehensive asset inventory shall be maintained
- The inventory shall include:
  - Information assets (data, documents, records)
  - Software assets (applications, systems, tools)
  - Physical assets (hardware, equipment, media)
  - Services (cloud services, utilities, outsourced services)
  - People (skills, qualifications, experience)
- The inventory shall be stored in a secure, accessible repository
- The inventory shall be kept current and accurate
- The inventory shall be reviewed and updated regularly

2.3 Asset Discovery

- Regular asset discovery activities shall be conducted
- Discovery methods may include:
  - Automated discovery tools
  - Physical inspections
  - Network scans
  - Documentation reviews
  - User surveys
- Undocumented assets shall be investigated and added to the inventory
- Discrepancies shall be resolved promptly

3. Asset Ownership and Responsibility

3.1 Asset Ownership

- All assets shall have an assigned owner
- Asset owners shall be responsible for:
  - Ensuring assets are inventoried and classified
  - Defining access rights to assets
  - Approving access to assets
  - Reviewing access rights periodically
  - Ensuring appropriate controls are implemented
  - Ensuring assets are properly maintained
  - Authorizing asset disposal
- Ownership shall be assigned at an appropriate level of management
- Ownership shall be documented in the asset inventory
- Ownership changes shall be managed and recorded

3.2 Asset Custodianship

- Asset custodians may be assigned for day-to-day management
- Custodians shall be responsible for:
  - Implementing required controls
  - Maintaining assets according to requirements
  - Monitoring asset status and condition
  - Reporting issues to asset owners
  - Following asset handling procedures
- Custodianship shall be documented in the asset inventory
- Custodianship changes shall be managed and recorded

3.3 User Responsibilities

- Users of assets shall be responsible for:
  - Using assets only for authorized purposes
  - Following asset handling procedures
  - Protecting assets from unauthorized access
  - Reporting security incidents involving assets
  - Returning assets when no longer required
- User responsibilities shall be documented
- Users shall acknowledge their responsibilities
- Users shall be held accountable for asset misuse

4. Asset Classification

4.1 Classification Scheme

- A classification scheme shall be established for information assets
- Classification shall be based on:
  - Confidentiality requirements
  - Integrity requirements
  - Availability requirements
  - Legal and regulatory requirements
  - Business value
  - Sensitivity
- Classification levels shall be clearly defined
- Classification shall determine protection requirements

4.2 Classification Levels

The following classification levels shall be used: - **[HIGHEST LEVEL]** (e.g., Confidential): Information that requires the highest level of protection due to severe impact if compromised - **[MEDIUM LEVEL]** (e.g., Internal): Information that requires protection but has moderate impact if compromised - **[LOWEST LEVEL]** (e.g., Public): Information that requires minimal protection and has minimal impact if compromised - Additional levels may be defined as needed

4.3 Classification Process

- Asset owners shall be responsible for classifying assets
- Classification shall be performed:
  - When assets are created or acquired
  - When assets are substantially modified
  - When business requirements change
  - During regular reviews
- Classification shall be documented in the asset inventory
- Classification shall be reviewed periodically
- Classification changes shall be managed and recorded

5. Asset Handling and Use

5.1 Handling Requirements

- Handling requirements shall be defined for each classification level
- Requirements shall address:
  - Access restrictions

    - Storage requirements
    - Transmission methods
    - Copying and printing
    - Labeling and marking
    - Physical security
    - Disposal methods
- Handling requirements shall be documented and communicated
- Compliance with handling requirements shall be monitored

5.2 Labeling and Marking

- Information assets shall be labeled according to classification
- Labeling shall be:
    - Clear and easily understood
    - Consistent across the organization
    - Appropriate to the medium
    - Durable and persistent
- Electronic documents shall include classification in headers/footers
- Physical documents shall be marked on each page
- Media shall be labeled externally
- Labeling exceptions shall be documented and approved

5.3 Information Storage

- Storage requirements shall be defined for each classification level
- Storage locations shall be appropriate to classification
- Sensitive information shall be stored securely
- Encryption shall be used for sensitive electronic information
- Physical information shall be stored in appropriate containers
- Backup storage shall meet the same requirements as primary storage
- Storage security shall be regularly assessed

5.4 Information Transmission

- Transmission requirements shall be defined for each classification level
- Secure transmission methods shall be used for sensitive information
- Encryption shall be used for transmitting sensitive information
- Physical transmission shall use appropriate secure methods
- Transmission security shall be regularly assessed
- Recipients shall be verified before transmission
- Transmission errors shall be reported and addressed

5.5 Information Reproduction

- Reproduction requirements shall be defined for each classification level
- Authorization may be required for reproducing sensitive information
- Reproduced information shall maintain original classification
- Unnecessary reproduction shall be avoided
- Reproduced copies shall be tracked where required
- Unused reproductions shall be securely disposed of
- Reproduction equipment shall be secured

6. Asset Lifecycle Management

6.1 Asset Acquisition

- Asset acquisition shall follow established procedures
- Security requirements shall be defined before acquisition
- Vendor security shall be assessed where appropriate
- Compliance with security requirements shall be verified
- Assets shall be registered in the inventory upon acquisition
- Initial classification shall be assigned
- Initial security controls shall be implemented

6.2 Asset Deployment

- Asset deployment shall follow established procedures
- Security configurations shall be applied before deployment
- Baseline security controls shall be implemented
- Deployment shall be documented
- User training shall be provided where necessary
- Deployment verification shall be performed
- Post-deployment security assessment shall be conducted

6.3 Asset Maintenance

- Assets shall be maintained according to requirements
- Maintenance shall include:
  - Regular updates and patches
  - Performance monitoring
  - Security assessments
  - Compliance verification
- Maintenance activities shall be documented
- Maintenance by third parties shall be supervised
- Maintenance effectiveness shall be regularly assessed

6.4 Asset Transfer

- Asset transfers shall be authorized and documented
- Transfers shall maintain appropriate security controls
- Classification shall be verified before transfer
- Recipients shall acknowledge receipt
- Inventory shall be updated after transfer
- Transfer methods shall be appropriate to classification
- International transfers shall comply with relevant regulations

6.5 Asset Disposal

- Asset disposal shall follow established procedures
- Disposal shall be authorized by asset owners
- Sensitive information shall be securely removed before disposal
- Disposal methods shall be appropriate to classification
- Disposal shall be documented
- Certificates of destruction shall be obtained where appropriate
- Disposal shall comply with environmental regulations
- Inventory shall be updated after disposal

7. Software Asset Management

7.1 Software Inventory

- All software assets shall be inventoried
- The inventory shall include:
  - Software name and version
  - License information
  - Installation locations
  - Owner and purpose
  - Support status
  - Security status
- The inventory shall be regularly updated
- Unauthorized software shall be identified and addressed

7.2 Software Licensing

- Software licensing compliance shall be maintained
- License terms shall be documented
- License usage shall be monitored
- License renewals shall be managed
- License audits shall be supported

- License violations shall be addressed promptly
- License documentation shall be securely stored

7.3 Software Security

- Software security shall be maintained throughout the lifecycle
- Security updates shall be applied promptly
- End-of-life software shall be identified and addressed
- Software vulnerabilities shall be monitored
- Security configurations shall be documented and maintained
- Software security shall be regularly assessed
- Security issues shall be promptly addressed

8. Hardware Asset Management

8.1 Hardware Inventory

- All hardware assets shall be inventoried
- The inventory shall include:
  - Hardware type and model
  - Serial number or asset tag
  - Location and status
  - Owner and purpose
  - Configuration information
  - Support status
- The inventory shall be regularly updated
- Unauthorized hardware shall be identified and addressed

8.2 Hardware Security

- Hardware security shall be maintained throughout the lifecycle
- Physical security controls shall be implemented
- Firmware updates shall be applied promptly
- Hardware vulnerabilities shall be monitored
- Security configurations shall be documented and maintained
- Hardware security shall be regularly assessed
- Security issues shall be promptly addressed

8.3 Mobile Devices

- Mobile devices shall be managed according to the Mobile Device Policy
- Mobile devices shall be inventoried
- Security controls shall be implemented on mobile devices

- Mobile device usage shall be monitored
- Lost or stolen devices shall be reported immediately
- Remote wipe capabilities shall be implemented where appropriate
- Mobile device security shall be regularly assessed

9. Media Management

9.1 Media Handling

- Media handling procedures shall be established
- Procedures shall address:
  - Storage requirements
  - Access restrictions
  - Transportation methods
  - Erasure and disposal
- Media shall be protected according to classification
- Media inventories shall be maintained where appropriate
- Media handling shall be regularly assessed

9.2 Media Erasure and Disposal

- Media erasure and disposal procedures shall be established
- Procedures shall be appropriate to classification
- Methods may include:
  - Secure deletion
  - Degaussing
  - Physical destruction
  - Specialized disposal services
- Erasure and disposal shall be verified
- Erasure and disposal shall be documented
- Certificates of destruction shall be obtained where appropriate

10. Asset Protection

10.1 Physical Protection

- Physical protection shall be appropriate to asset value and classification
- Protection measures may include:
  - Access controls
  - Secure storage
  - Environmental controls
  - Monitoring and surveillance

    - Theft prevention
- Protection effectiveness shall be regularly assessed
- Protection incidents shall be investigated
- Protection improvements shall be implemented as needed

10.2 Technical Protection

- Technical protection shall be appropriate to asset value and classification
- Protection measures may include:
    - Access controls
    - Encryption
    - Backup and recovery
    - Malware protection
    - Monitoring and logging
- Protection effectiveness shall be regularly assessed
- Protection incidents shall be investigated
- Protection improvements shall be implemented as needed

10.3 Administrative Protection

- Administrative protection shall be appropriate to asset value and classification
- Protection measures may include:
    - Policies and procedures
    - Training and awareness
    - Risk assessments
    - Compliance monitoring
    - Auditing and review
- Protection effectiveness shall be regularly assessed
- Protection incidents shall be investigated
- Protection improvements shall be implemented as needed

11. Asset Monitoring and Compliance

11.1 Asset Monitoring

- Assets shall be monitored for:
    - Usage and performance
    - Security status
    - Compliance with policies
    - Unauthorized changes
    - Unusual activities
- Monitoring shall be appropriate to asset value and classification
- Monitoring results shall be regularly reviewed

- Issues identified through monitoring shall be addressed

11.2 Asset Auditing

- Asset audits shall be conducted regularly
- Audits shall verify:
  - Inventory accuracy
  - Classification appropriateness
  - Control implementation
  - Compliance with policies
  - User awareness
- Audit findings shall be documented
- Corrective actions shall be implemented
- Audit effectiveness shall be assessed

11.3 Compliance Verification

- Asset management compliance shall be regularly verified
- Verification shall address:
  - Policy compliance
  - Regulatory compliance
  - Contractual compliance
  - Standard compliance
- Non-compliance shall be addressed through appropriate channels
- Compliance trends shall be analyzed
- Compliance improvements shall be implemented

12. Roles and Responsibilities

12.1 Management

- Approve the Asset Management Policy
- Provide resources for asset management
- Review asset management performance
- Address significant asset management issues
- Support asset management initiatives
- Ensure compliance with requirements

12.2 Asset Owners

- Ensure assets are properly inventoried
- Classify assets appropriately
- Define access rights to assets

- Ensure appropriate controls are implemented
- Review asset status regularly
- Authorize asset disposal
- Report significant asset issues

12.3 Asset Custodians

- Implement required controls
- Maintain assets according to requirements
- Monitor asset status and condition
- Report issues to asset owners
- Follow asset handling procedures
- Support asset audits and assessments
- Implement corrective actions

12.4 Information Security Team

- Develop and maintain the Asset Management Policy
- Provide guidance on asset classification
- Advise on security controls for assets
- Monitor asset security compliance
- Investigate security incidents involving assets
- Recommend security improvements
- Report on asset security status

12.5 IT Department

- Maintain hardware and software inventories
- Implement technical controls for assets
- Support asset discovery activities
- Manage software licensing
- Implement secure disposal of electronic assets
- Support asset monitoring
- Provide technical expertise for asset management

12.6 All Users

- Use assets only for authorized purposes
- Follow asset handling procedures
- Protect assets from unauthorized access
- Report security incidents involving assets
- Return assets when no longer required
- Participate in asset management training
- Support asset audits and assessments

13. 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

14. Related Documents

- Information Security Policy
- Information Classification Policy
- Access Control Policy
- Mobile Device Policy
- Media Handling Procedure
- Asset Disposal Procedure
- [LIST OTHER RELEVANT POLICIES AND PROCEDURES]

15. Approval

This Asset Management Policy is approved by:

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