Information Classification Policy Template

Document Control Information

- **Document Title:** Information Classification 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 Information Classification Policy establishes [ORGANIZATION NAME]'s approach to classifying and handling information assets in accordance with ISO 27001:2022 requirements. It provides a framework for ensuring that information receives an appropriate level of protection according to its sensitivity, criticality, and value to the organization.

1.2 Scope

This policy applies to all information assets owned, controlled, or processed by [ORGANIZATION NAME], regardless of format or medium, including: - Electronic data and documents - Physical documents and records - Databases and structured data - Email and messaging content - Audio and video recordings - System configurations and code - Backup media and archives

1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Classifying information assets according to their sensitivity, criticality, and value - Implementing appropriate controls based on classification levels - Ensuring information is handled in accordance with its classification - Regularly reviewing and updating information classifications - Training personnel on information classification and handling requirements

2. Information Classification Framework

2.1 Classification Criteria

Information shall be classified based on: - Confidentiality requirements - Integrity requirements - Availability requirements - Legal, regulatory, and contractual obligations - Business value and operational importance - Potential impact if compromised

2.2 Classification Levels

[ORGANIZATION NAME] shall use the following classification levels:

2.2.1 Public

- Information officially approved for public release
- No restrictions on disclosure
- Disclosure would cause no harm to the organization
- Examples: Marketing materials, public website content, press releases

2.2.2 Internal

- Information intended for use within the organization
- Not approved for public release
- Limited business impact if disclosed
- Examples: Internal announcements, general procedures, non-sensitive project documentation

2.2.3 Confidential

- Sensitive information with restricted distribution
- Unauthorized disclosure could cause moderate harm to the organization
- Access limited to specific groups or roles
- Examples: Financial data, employee records, business strategies, customer information

2.2.4 Restricted

- Highly sensitive information requiring the strictest protection
- Unauthorized disclosure could cause severe harm to the organization
- Access limited to named individuals with specific need-to-know
- Examples: Trade secrets, merger and acquisition plans, authentication credentials, security infrastructure details

3. Classification Responsibilities

3.1 Information Owners

- Determine the appropriate classification level for information assets
- Review and update classifications periodically
- Authorize access to classified information
- Ensure appropriate controls are implemented

3.2 Information Custodians

- Implement and maintain controls according to classification levels
- Store and process information in accordance with its classification
- Monitor and report on compliance with classification requirements

3.3 Information Users

- Handle information according to its classification level
- Respect access restrictions and handling requirements
- Report suspected misclassification or security incidents
- Seek clarification when classification is unclear

4. Information Labeling and Handling

4.1 Labeling Requirements

4.1.1 Electronic Information

- Classification shall be clearly indicated in document headers/footers
- Classification shall be included in file names where practical
- Classification shall be indicated in email subject lines where appropriate
- System-generated labels shall be applied where possible

4.1.2 Physical Information

- Classification shall be clearly marked on the front cover
- Classification shall be indicated on each page where practical
- Classification shall be visible on storage containers and media
- Color-coding may be used to enhance visibility of classification

4.2 Handling Requirements

4.2.1 Public Information

- May be freely distributed without restrictions
- No special handling requirements
- May be published on public websites and social media
- No approval required for distribution

4.2.2 Internal Information

- Distribution limited to employees and authorized contractors
- May be stored on internal systems without encryption
- Should not be posted on public websites or social media
- May be discussed in internal meetings and spaces

4.2.3 Confidential Information

- Distribution limited to authorized individuals with business need
- Must be encrypted when transmitted electronically
- Must be stored in secure locations or encrypted when stored electronically
- Must not be discussed in public places
- Must be disposed of securely when no longer needed

4.2.4 Restricted Information

- Distribution strictly limited to named individuals
- Must be encrypted with strong encryption when stored or transmitted
- Must be stored in highly secure locations with access controls
- Must be tracked throughout its lifecycle
- Must be disposed of using secure destruction methods
- Must not be copied without explicit authorization

5. Information Exchange and Transfer

5.1 Internal Exchange

- Information shall only be shared with individuals authorized to access it
- Classification level shall be clearly communicated when sharing information
- Appropriate methods shall be used based on classification level

5.2 External Exchange

- Information shall only be shared with external parties when authorized
- Confidentiality agreements shall be in place before sharing sensitive information
- Secure transfer methods shall be used based on classification level
- External recipients shall be informed of classification and handling requirements

5.3 Secure Transfer Methods

- Public: Standard methods without encryption
- Internal: Corporate email or file sharing systems
- Confidential: Encrypted email, secure file transfer, or encrypted media
- Restricted: Strong encryption with secure key exchange, secure courier for physical media

6. Information Storage and Disposal

6.1 Storage Requirements

- Public: No special storage requirements
- Internal: Access limited to employees and authorized contractors
- Confidential: Secure storage with access controls, encryption recommended
- Restricted: Encrypted storage with strong access controls, activity logging

6.2 Backup Requirements

- Backups shall maintain the same classification level as the original information
- Backup media shall be labeled and protected according to the highest classification level of contained information
- Encryption shall be used for backups containing confidential or restricted information

6.3 Disposal Requirements

- Public: Normal disposal
- Internal: Basic destruction (e.g., shredding, secure deletion)
- Confidential: Secure destruction using approved methods
- Restricted: Verified secure destruction with documentation

7. Reclassification and Declassification

7.1 Reclassification Process

- Information owners may change classification levels as needed
- Reclassification shall be documented with justification
- All copies of reclassified information shall be updated
- Users shall be notified of significant classification changes

7.2 Declassification Process

- Information may be declassified when sensitivity decreases
- Declassification shall be approved by the information owner
- Declassification shall be documented with justification
- Declassified information shall be relabeled appropriately

7.3 Periodic Review

- Classification levels shall be reviewed periodically
- Review frequency shall be based on information sensitivity
- Reviews shall consider changes in business context and threats

8. Training and Awareness

8.1 Employee Training

- All employees shall receive training on information classification
- Training shall cover classification levels and handling requirements
- Training shall be provided during onboarding and refreshed annually

8.2 Specialized Training

- Information owners and custodians shall receive specialized training
- Personnel handling highly sensitive information shall receive additional training
- Training shall be updated when classification requirements change

9. Compliance and Monitoring

9.1 Compliance Verification

- Regular audits shall verify compliance with this policy
- Spot checks may be conducted on information handling practices
- Systems shall be configured to enforce classification controls where possible

9.2 Non-Compliance

- Incidents of non-compliance shall be reported and investigated
- Corrective actions shall be implemented as needed
- Disciplinary action may result from willful non-compliance

10. Exceptions

Exceptions to this policy shall be: - Documented with justification - Approved by the information owner and security officer - Time-limited and regularly reviewed - Accompanied by compensating controls where appropriate

11. Related Documents

- Information Security Policy
- Data Protection Policy
- Access Control Policy
- Information Handling Procedures
- Secure Disposal Procedures
- [LIST OTHER RELEVANT POLICIES AND PROCEDURES]

12. Approval

This Information Classification Policy is approved by:

Name: _______________________ Position: _____________________ Date: ________________________ Signature: ____________________