Data Classification and Handling Policy Template

Document Control Information

- **Document Title:** Data Classification and Handling 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 Data Classification and Handling Policy establishes [ORGANIZATION NAME]'s requirements for classifying and handling information assets based on their sensitivity, value, and criticality in accordance with ISO 27001:2022 requirements. It provides a framework for ensuring that information receives appropriate protection throughout its lifecycle.

1.2 Scope

This policy applies to: - All information assets owned, processed, stored, or transmitted by [ORGANIZATION NAME] - All forms of information, including electronic, physical, and verbal - All information systems and applications that process or store information - All employees, contractors, consultants, and third parties who access organizational information - All locations where organizational information is processed or stored

1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Classifying information assets according to their sensitivity, value, and criticality - Implementing appropriate controls based on information classification - Handling information in accordance with its classification level - Protecting information throughout its lifecycle - Ensuring that information is accessible only to authorized individuals - Complying with relevant legal, regulatory, and contractual requirements - Regularly reviewing and updating classification and handling procedures

2. Data Classification Framework

2.1 Classification Levels

The following classification levels shall be used:

2.1.1 [HIGHEST LEVEL] (e.g., Confidential)

Information that requires the highest level of protection due to its sensitivity, value, or criticality. Unauthorized disclosure, modification, or destruction of this information would cause severe damage to the organization, its customers, partners, or employees.

Examples: - Strategic business plans - Merger and acquisition information - Sensitive financial information - Authentication credentials - Sensitive personal data - Intellectual property - [CUSTOMIZE BASED ON ORGANIZATIONAL NEEDS]

2.1.2 [MEDIUM LEVEL] (e.g., Internal)

Information that requires protection but has moderate sensitivity, value, or criticality. Unauthorized disclosure, modification, or destruction of this information would cause significant but not severe damage to the organization, its customers, partners, or employees.

Examples: - Internal procedures and processes - Non-sensitive business information - General employee information - Internal communications - Project documentation - [CUSTOMIZE BASED ON ORGANIZATIONAL NEEDS]

2.1.3 [LOWEST LEVEL] (e.g., Public)

Information that requires minimal protection and can be disclosed publicly. Unauthorized disclosure, modification, or destruction of this information would cause minimal or no damage to the organization, its customers, partners, or employees.

Examples: - Marketing materials - Public announcements - Published research - Product information - Job postings - [CUSTOMIZE BASED ON ORGANIZATIONAL NEEDS]

2.2 Classification Criteria

Information shall be classified based on the following criteria:

2.2.1 Confidentiality

- Impact of unauthorized disclosure
- Legal, regulatory, or contractual requirements
- Privacy considerations
- Business sensitivity

2.2.2 Integrity

- Impact of unauthorized modification
- Accuracy requirements
- Authenticity requirements
- Reliability requirements

2.2.3 Availability

- Impact of unavailability
- Recovery time requirements
- Business continuity needs
- Operational importance

2.2.4 Value

- Business value
- Competitive advantage
- Replacement cost
- Strategic importance

3. Classification Process

3.1 Initial Classification

- Information shall be classified at creation or acquisition
- Classification shall be performed by information owners
- Classification shall consider all relevant criteria
- Classification shall be documented
- Classification shall be communicated to users
- Default classification shall be [MEDIUM LEVEL] when uncertain
- Classification shall be reviewed by information security when needed

3.2 Classification Review

- Classification shall be reviewed periodically

- Review frequency shall be based on information sensitivity
- Review shall be performed by information owners
- Review shall consider changes in:
    - Information content
    - Business value
    - Legal requirements
    - Risk landscape
- Classification changes shall be documented
- Classification changes shall be communicated to users
- Review shall be documented

3.3 Reclassification

- Information shall be reclassified when necessary
- Reclassification shall be performed by information owners
- Reclassification shall be documented
- Reclassification shall be communicated to users
- Controls shall be adjusted based on new classification
- Reclassification shall be reviewed by information security when needed
- Reclassification history shall be maintained

4. Labeling and Marking

4.1 Electronic Information

- Electronic information shall be labeled according to classification
- Labeling shall be:
    - Clear and visible
    - Consistent across the organization
    - Appropriate to the medium
    - Automated where possible
- Labeling methods may include:
    - Document headers/footers
    - File naming conventions
    - Metadata
    - System tags
    - Visual indicators
- Labeling exceptions shall be documented and approved

4.2 Physical Information

- Physical information shall be marked according to classification

- Marking shall be:
  - Clear and visible
  - Consistent across the organization
  - Appropriate to the medium
  - Durable
- Marking methods may include:
  - Headers/footers
  - Cover sheets
  - Labels
  - Stamps
  - Colored paper
- Marking exceptions shall be documented and approved

4.3 Verbal Information

- Verbal communication of classified information shall be controlled
- Controls may include:
  - Verbal classification announcements
  - Meeting confidentiality statements
  - Non-disclosure agreements
  - Location restrictions
  - Participant restrictions
- Verbal communication controls shall be appropriate to classification
- Verbal communication guidance shall be provided to staff

5. Handling Requirements

5.1 [HIGHEST LEVEL] Handling

- Access shall be strictly limited to authorized individuals with a need to know
- Authentication shall use multi-factor methods where possible
- Transmission shall use strong encryption
- Storage shall use encryption
- Physical copies shall be stored in secured locations
- Distribution shall be tracked and logged
- Disposal shall use secure destruction methods
- Working copies shall be protected and tracked
- Remote access shall have additional controls
- Printing shall be restricted and controlled
- Mobile device usage shall be restricted
- Third-party sharing shall require approval and agreements
- [CUSTOMIZE BASED ON ORGANIZATIONAL NEEDS]

5.2 [MEDIUM LEVEL] Handling

- Access shall be limited to authorized individuals
- Authentication shall use standard methods
- Transmission shall use encryption when outside the organization
- Storage shall follow standard security practices
- Physical copies shall be stored in controlled locations
- Distribution shall be to authorized recipients only
- Disposal shall follow secure disposal procedures
- Working copies shall be controlled
- Remote access shall follow standard security practices
- Printing shall follow standard procedures
- Mobile device usage shall follow standard security practices
- Third-party sharing shall require agreements
- [CUSTOMIZE BASED ON ORGANIZATIONAL NEEDS]

5.3 [LOWEST LEVEL] Handling

- Access may be provided to the general public
- Authentication may not be required
- Transmission may use standard methods
- Storage shall follow standard practices
- Physical copies may be stored in standard locations
- Distribution may be unrestricted
- Disposal shall follow standard procedures
- Working copies do not require special controls
- Remote access may follow standard practices
- Printing may follow standard procedures
- Mobile device usage may follow standard practices
- Third-party sharing may be permitted
- [CUSTOMIZE BASED ON ORGANIZATIONAL NEEDS]

6. Access Control

6.1 Access Principles

- Access shall be based on classification level
- Access shall follow the principle of least privilege
- Access shall be granted on a need-to-know basis
- Access shall be regularly reviewed
- Access shall be promptly revoked when no longer needed
- Access shall be documented and approved
- Access shall be monitored and logged

6.2 Authentication Requirements

- Authentication strength shall be appropriate to classification
- [HIGHEST LEVEL] information shall require strong authentication
- [MEDIUM LEVEL] information shall require standard authentication
- [LOWEST LEVEL] information may not require authentication
- Authentication methods shall be regularly reviewed
- Authentication failures shall be monitored and addressed
- Authentication requirements shall be documented

6.3 Authorization Requirements

- Authorization shall be required for access to classified information
- Authorization shall be provided by information owners
- Authorization shall be documented
- Authorization shall be time-limited where appropriate
- Authorization shall be regularly reviewed
- Authorization shall be promptly revoked when no longer needed
- Authorization requirements shall be documented

7. Storage and Transmission

7.1 Storage Requirements

- Storage security shall be appropriate to classification
- [HIGHEST LEVEL] information shall be stored with enhanced security
- [MEDIUM LEVEL] information shall be stored with standard security
- [LOWEST LEVEL] information shall be stored with basic security
- Storage locations shall be appropriate to classification
- Storage methods shall be documented
- Storage security shall be regularly assessed
- Storage requirements shall be communicated to users

7.2 Transmission Requirements

- Transmission security shall be appropriate to classification
- [HIGHEST LEVEL] information shall be transmitted with enhanced security
- [MEDIUM LEVEL] information shall be transmitted with standard security
- [LOWEST LEVEL] information shall be transmitted with basic security
- Transmission methods shall be appropriate to classification
- Transmission security shall be regularly assessed
- Transmission requirements shall be documented
- Transmission requirements shall be communicated to users

7.3 Encryption Requirements

- Encryption shall be used based on classification
- [HIGHEST LEVEL] information shall require encryption in transit and at rest
- [MEDIUM LEVEL] information shall require encryption in transit outside the organization
- [LOWEST LEVEL] information may not require encryption
- Encryption methods shall use approved algorithms and key lengths
- Encryption keys shall be securely managed
- Encryption requirements shall be documented
- Encryption effectiveness shall be regularly assessed

8. Reproduction and Distribution

8.1 Reproduction Controls

- Reproduction shall be controlled based on classification
- [HIGHEST LEVEL] information reproduction shall be restricted and logged
- [MEDIUM LEVEL] information reproduction shall follow standard controls
- [LOWEST LEVEL] information reproduction may not be restricted
- Reproduction methods shall be appropriate to classification
- Reproduction shall maintain original classification
- Reproduction controls shall be documented
- Reproduction controls shall be communicated to users

8.2 Distribution Controls

- Distribution shall be controlled based on classification
- [HIGHEST LEVEL] information distribution shall be restricted and logged
- [MEDIUM LEVEL] information distribution shall follow standard controls
- [LOWEST LEVEL] information distribution may not be restricted
- Distribution methods shall be appropriate to classification
- Distribution shall include classification markings
- Distribution controls shall be documented
- Distribution controls shall be communicated to users

8.3 Tracking Requirements

- Information tracking shall be based on classification
- [HIGHEST LEVEL] information shall be tracked throughout its lifecycle
- [MEDIUM LEVEL] information may require limited tracking
- [LOWEST LEVEL] information may not require tracking
- Tracking methods shall be appropriate to classification

- Tracking shall include key events and transfers
- Tracking requirements shall be documented
- Tracking effectiveness shall be regularly assessed

9. Disposal and Destruction

9.1 Retention Requirements

- Retention shall comply with legal, regulatory, and business requirements
- Retention periods shall be defined for each classification level
- Retention shall be documented
- Retention shall be monitored
- Retention exceptions shall be approved and documented
- Retention requirements shall be communicated to users
- Retention compliance shall be regularly assessed

9.2 Disposal Methods

- Disposal methods shall be appropriate to classification
- [HIGHEST LEVEL] information shall require secure destruction
- [MEDIUM LEVEL] information shall require controlled disposal
- [LOWEST LEVEL] information may use standard disposal
- Disposal shall be documented where required
- Disposal methods shall be regularly assessed
- Disposal requirements shall be communicated to users
- Disposal compliance shall be regularly verified

9.3 Destruction Verification

- Destruction verification shall be based on classification
- [HIGHEST LEVEL] information destruction shall be verified and documented
- [MEDIUM LEVEL] information destruction may require verification
- [LOWEST LEVEL] information destruction may not require verification
- Verification methods shall be appropriate to classification
- Verification shall be documented where required
- Verification requirements shall be communicated to users
- Verification effectiveness shall be regularly assessed

10. Third-Party Sharing

10.1 Sharing Requirements

- Information sharing shall be based on classification

- [HIGHEST LEVEL] information sharing shall require approval and agreements
- [MEDIUM LEVEL] information sharing shall require agreements
- [LOWEST LEVEL] information sharing may not require special controls
- Sharing shall be documented where required
- Sharing shall include classification and handling requirements
- Sharing requirements shall be communicated to users
- Sharing compliance shall be regularly assessed

10.2 Third-Party Controls

- Third parties shall implement controls appropriate to classification
- Controls shall be verified before sharing [HIGHEST LEVEL] information
- Controls shall be documented in agreements
- Controls shall be regularly assessed
- Control deficiencies shall be addressed
- Control requirements shall be communicated to third parties
- Control compliance shall be regularly verified

10.3 Non-Disclosure Agreements

- NDAs shall be required based on classification
- [HIGHEST LEVEL] information sharing shall require NDAs
- [MEDIUM LEVEL] information sharing may require NDAs
- [LOWEST LEVEL] information sharing may not require NDAs
- NDAs shall be reviewed by legal
- NDAs shall be maintained and tracked
- NDA requirements shall be communicated to users
- NDA compliance shall be regularly verified

11. Incident Management

11.1 Classification Incidents

- Classification incidents shall be promptly reported
- Incidents may include:
    - Misclassification
    - Missing classification
    - Classification conflicts
    - Classification errors
- Incidents shall be investigated
- Corrective actions shall be implemented
- Incidents shall be documented
- Incident trends shall be analyzed

- Incident response shall be appropriate to classification

11.2 Handling Incidents

- Handling incidents shall be promptly reported
- Incidents may include:
  - Unauthorized access
  - Improper handling
  - Control failures
  - Procedure violations
- Incidents shall be investigated
- Corrective actions shall be implemented
- Incidents shall be documented
- Incident trends shall be analyzed
- Incident response shall be appropriate to classification

11.3 Breach Response

- Information breaches shall be managed according to the Incident Management Policy
- Response shall be appropriate to classification
- [HIGHEST LEVEL] information breaches shall receive highest priority
- [MEDIUM LEVEL] information breaches shall receive standard priority
- [LOWEST LEVEL] information breaches shall receive routine priority
- Response shall include containment, eradication, and recovery
- Response shall be documented
- Response effectiveness shall be assessed
- Lessons learned shall be incorporated into controls

12. Training and Awareness

12.1 Classification Training

- All staff shall receive classification training
- Training shall cover:
  - Classification levels
  - Classification criteria
  - Classification process
  - Classification responsibilities
- Training shall be provided at onboarding and regularly thereafter
- Training shall be appropriate to job responsibilities
- Training completion shall be documented
- Training effectiveness shall be assessed

- Training materials shall be regularly updated

12.2 Handling Training

- All staff shall receive handling training
- Training shall cover:
  - Handling requirements for each classification level
  - Labeling and marking
  - Storage and transmission
  - Reproduction and distribution
  - Disposal and destruction
- Training shall be provided at onboarding and regularly thereafter
- Training shall be appropriate to job responsibilities
- Training completion shall be documented
- Training effectiveness shall be assessed
- Training materials shall be regularly updated

12.3 Awareness Program

- A classification and handling awareness program shall be maintained
- The program shall include:
  - Regular communications
  - Visual reminders
  - Practical examples
  - Common mistakes
  - Incident lessons learned
- Awareness shall be reinforced through multiple channels
- Awareness effectiveness shall be assessed
- Awareness materials shall be regularly updated
- Awareness shall be integrated into organizational culture

13. Roles and Responsibilities

13.1 Information Owners

- Classify information assets
- Review and update classification
- Authorize access to information
- Ensure appropriate controls are implemented
- Approve information sharing
- Report classification incidents
- Ensure compliance with this policy
- Provide input to classification standards

13.2 Information Custodians

- Implement classification controls
- Apply and maintain labels and markings
- Manage information storage and transmission
- Control information reproduction and distribution
- Execute disposal and destruction
- Report handling incidents
- Support classification reviews
- Follow handling requirements

13.3 Information Security Team

- Develop and maintain this policy
- Provide classification and handling guidance
- Review classification for high-value assets
- Monitor compliance with this policy
- Investigate classification and handling incidents
- Coordinate training and awareness
- Report on classification and handling status
- Recommend control improvements

13.4 All Users

- Follow classification and handling requirements
- Apply appropriate labels and markings
- Report classification and handling incidents
- Protect information according to classification
- Complete required training
- Suggest classification and handling improvements
- Maintain awareness of requirements
- Ask questions when uncertain

14. Compliance and Exceptions

14.1 Compliance Monitoring

- Compliance with this policy shall be regularly monitored
- Monitoring methods may include:
    - Periodic reviews
    - Spot checks
    - Automated scanning
    - Self-assessments

    - Audits
- Non-compliance shall be addressed
- Compliance trends shall be analyzed
- Compliance reports shall be provided to management
- Compliance monitoring shall be documented

14.2 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 - Tracked and reported - Minimized to the extent possible - Consistent with legal and regulatory requirements

15. Related Documents

- Information Security Policy
- Access Control Policy
- Data Protection Policy
- Incident Management Policy
- Third-Party Security Policy
- Records Management Policy
- [LIST OTHER RELEVANT POLICIES AND PROCEDURES]

16. Approval

This Data Classification and Handling Policy is approved by:

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