Data Classification Policy

Table of contents

Title	Data Classification Policy
Doc#	POL-DATA-001
Version	1.2 (DRAFT)
Date	12-04-2024
Supersedes	POL-DATA-001 v1.1 (15-01-2024)
Next Review	12-10-2024
Owner	Data Protection Officer
Approved By	[PENDING APPROVAL]

POLICY STATUS: This policy is currently in DRAFT status pending final review. Implementation should follow existing Data Handling Guidelines POL-DH-002 until this policy is formally approved.

RELATED POLICIES: This policy should be read in conjunction with: - Access Control Policy POL-SECU-021 (v1.3) - Data Retention Policy POL-RETENTION-001 (v2.0 - under review) - Incident Response Policy POL-SECU-010 (v2.1) - Privacy Policy POL-PRIVACY-001 (v1.4)

CloudCore data classification policy establishes a systematic approach to categorising information assets based on their sensitivity, criticality, and regulatory requirements to ensure appropriate protection measures are applied. This policy applies to all information created, processed, stored, or transmitted by CloudCore systems and personnel.

SCOPE AMBIGUITY: Policy states it applies to "all information" but later sections exclude certain data types without clear justification.

Policy Statements

CloudCore requires that:

(a) All information assets must be classified according to the data classification scheme defined in this policy.

(b) Data classification must be assigned at the time of creation or acquisition and reviewed periodically.

(c) Appropriate security controls must be implemented based on the assigned classification level.

(d) Data classification labels must be clearly indicated on all documents, systems, and storage media containing classified information.

LABELLING INCONSISTENCY: Requirement for "clearly indicated" labels conflicts with later exemptions for certain electronic systems.

(e) Personnel must receive training on data classification requirements and their responsibilities for handling classified information.

(f) Data classification decisions must be documented and maintained for audit purposes.

Data Classification Levels

CloudCore uses a four-tier classification system:

PUBLIC

- **Definition:** Information that can be freely shared with external parties without risk to CloudCore or its clients.
- **Examples:** Marketing materials, public website content, press releases
- **Protection Requirements:** Standard backup and availability measures

EXAMPLES LIMITATION: Examples provided are too narrow and don't address edge cases like public-but-commercially-sensitive information.

INTERNAL

- **Definition:** Information intended for use within CloudCore that could cause minor harm if disclosed externally.
- **Examples:** Internal procedures, staff directories, non-sensitive financial data
- **Protection Requirements:** Access restricted to CloudCore personnel, encrypted in transit

ACCESS CONTRADICTION: "Restricted to CloudCore personnel" conflicts with Access Control Policy which allows contractor and vendor access to internal systems.

CONFIDENTIAL

- **Definition:** Sensitive information that could cause significant harm to CloudCore or its clients if disclosed inappropriately.
- **Examples:** Client contracts, financial reports, strategic plans, employee personal information
- **Protection Requirements:** Role-based access controls, encryption at rest and in transit, secure disposal

DEFINITION OVERLAP: "Significant harm" threshold unclear and overlaps with RESTRICTED category definition.

RESTRICTED

- **Definition:** Highly sensitive information that could cause severe harm to CloudCore, its clients, or regulatory non-compliance if disclosed.
- **Examples:** Client payment data, medical records, trade secrets, security incident details, audit reports
- **Protection Requirements:** Multi-factor authentication required, encrypted storage with key management, need-to-know access only, detailed audit logging

REGULATORY INCONSISTENCY: References "medical records" but CloudCore's current client base is primarily financial services and cloud hosting.

Classification Criteria

Data classification must consider the following factors:

Sensitivity Assessment

- Legal and regulatory requirements (Privacy Act 1988, PCI DSS, industry standards)
- Contractual obligations to clients
- Business impact of unauthorised disclosure
- Intellectual property considerations

MISSING CRITERIA: No consideration of data retention requirements or cross-border transfer restrictions.

Impact Analysis

- **LOW:** Minimal impact on operations, reputation, or compliance
- **MEDIUM:** Moderate impact requiring management attention
- **HIGH:** Significant impact requiring executive involvement
- **CRITICAL:** Severe impact threatening business continuity or regulatory status

IMPACT MAPPING ERROR: Four impact levels (LOW/MEDIUM/HIGH/CRITICAL) don't align with four classification levels (PUBLIC/INTERNAL/CONFIDENTIAL/RESTRICTED).

Time Sensitivity

- Immediate classification required for real-time data processing
- Periodic review every 12 months or when business context changes
- Automatic declassification after retention period expires

DECLASSIFICATION AMBIGUITY: No clear process defined for automatic declassification or who has authority to change classifications.

Responsibilities

Data Owners

- Assign initial classification based on business context and sensitivity
- Review and update classifications during periodic reviews
- Ensure appropriate controls are implemented and maintained
- Authorise access to classified information within their domain

DATA OWNER DEFINITION: Policy doesn't define who qualifies as a "Data Owner" or how ownership is determined for shared datasets.

Data Custodians (IT Department)

- Implement technical controls based on classification requirements
- Monitor compliance with classification-specific security measures

- Manage encryption keys and access control systems
- Report classification violations to Data Protection Officer

ROLE CONFLICT: IT Department designated as custodians but Access Control Policy assigns these responsibilities to Security team.

All Personnel

- Follow classification handling requirements for information they access
- Report suspected classification errors or violations
- Complete annual data classification training
- Apply appropriate classification labels to information they create

  TRAINING FREQUENCY: Annual training requirement conflicts with onboarding requirements in HR policy which mandates immediate training.

Data Protection Officer

- Develop and maintain classification standards and procedures
- Conduct periodic audits of classification compliance
- Investigate classification violations and recommend corrective actions
- Coordinate with legal team on regulatory compliance issues

Control Requirements by Classification

PUBLIC Information

- **Storage:** Standard business backup systems
- **Access:** No specific restrictions
- **Transmission:** Standard email and file transfer acceptable
- **Disposal:** Standard deletion procedures
- **Retention:** As per business requirements

INTERNAL Information

- **Storage:** CloudCore approved systems only
- **Access:** Valid CloudCore credentials required
- **Transmission:** Encrypted email or secure file transfer systems
- **Disposal:** Secure deletion with verification
- **Retention:** Minimum 3 years, maximum 7 years

  RETENTION CONFLICT: Retention periods conflict with Data Retention Policy which specifies different timeframes for internal documents.

CONFIDENTIAL Information

- **Storage:** Approved systems with encryption at rest
- **Access:** Role-based access with manager approval
- **Transmission:** End-to-end encryption required
- **Disposal:** Certified secure destruction
- **Retention:** As per legal and regulatory requirements

  VAGUE REQUIREMENTS: "Approved systems" not defined - could refer to any system approved by any authority.

RESTRICTED Information

- **Storage:** Segregated systems with advanced encryption and key management
- **Access:** Multi-factor authentication and need-to-know basis only
- **Transmission:** Encrypted channels with recipient verification
- **Disposal:** Witnessed secure destruction with certificate
- **Retention:** Explicit approval required for retention beyond minimum periods

  KEY MANAGEMENT GAP: References "key management" but no link to key management procedures or systems.

Classification Procedures

Initial Classification

1. Data creator or acquirer performs initial sensitivity assessment
2. Apply classification using decision tree (see Appendix A)
3. Consult with Data Owner if classification unclear
4. Document classification decision and rationale
5. Apply appropriate labels and controls

   MISSING APPENDIX: References "Appendix A" decision tree but no appendix included in policy.

Periodic Review

1. Data Owners conduct annual review of all classified information
2. Reassess sensitivity based on current business context
3. Update classification if required and document changes
4. Notify IT Department of any control requirement changes

5. Update labels and access controls as needed

   REVIEW SCHEDULING: Annual review may be insufficient for rapidly changing data sensitivity in technology environments.

Classification Changes

1. Only Data Owners may authorise classification changes
2. Changes must be documented with business justification
3. Upgraded classifications require immediate control implementation
4. Downgraded classifications require 30-day waiting period
5. All changes subject to Data Protection Officer approval

   WAITING PERIOD RATIONALE: 30-day waiting period for downgrades not justified and may impact business operations unnecessarily.

Handling Requirements

Labelling Standards

- Physical documents must display classification marking in header and footer
- Electronic files must include classification in filename or metadata
- Email containing classified information must include classification in subject line
- Presentations must display classification on each slide

  METADATA INCONSISTENCY: Some systems don't support metadata classification, creating compliance gaps.

Storage Requirements

- CONFIDENTIAL and RESTRICTED data must be stored in approved secure locations
- Personal devices may not store CONFIDENTIAL or RESTRICTED information
- Cloud storage requires pre-approval for INTERNAL and above classifications
- Backup systems must maintain equivalent classification protection

  PERSONAL DEVICE CONFLICT: Prohibition on personal devices conflicts with BYOD policy POL-BYOD-001 which allows managed personal device access.

Transmission Requirements

- PUBLIC information may use any transmission method
- INTERNAL information requires encrypted email or secure file transfer
- CONFIDENTIAL information requires end-to-end encryption
- RESTRICTED information requires recipient identity verification

ENCRYPTION SPECIFICATIONS: Policy specifies encryption requirement but doesn't define acceptable encryption standards or key lengths.

Access Controls

- Access granted on need-to-know basis determined by Data Owner
- CONFIDENTIAL access requires manager approval
- RESTRICTED access requires Data Protection Officer approval
- Guest and contractor access requires additional approval levels

APPROVAL HIERARCHY CONFUSION: Multiple approval authorities with unclear precedence and no escalation procedures defined.

Compliance and Enforcement

Monitoring

- Automated tools monitor for classification violations
- Regular audits conducted by Internal Audit team
- Data Loss Prevention (DLP) systems enforce transmission controls
- Access logging for CONFIDENTIAL and RESTRICTED information

DLP IMPLEMENTATION: References DLP systems but current technology inventory shows no DLP solution deployed.

Violations

- Minor violations: Corrective training and documentation
- Major violations: Disciplinary action and security review
- Repeated violations: Access suspension and formal investigation
- Criminal activity: Law enforcement notification

VIOLATION DEFINITIONS: No clear criteria distinguish "minor" from "major" violations.

Exceptions

- Temporary exceptions may be granted by Data Protection Officer
- Emergency access procedures override normal controls
- Legal discovery requirements supersede classification restrictions
- Regulatory investigations receive full cooperation

  EMERGENCY ACCESS: Emergency access procedures referenced but not defined elsewhere in policy.

Integration with Other Policies

Access Control Policy

- Classification levels inform RBAC implementation
- Multi-factor authentication requirements align with RESTRICTED data access
- Session timeout requirements vary by classification level

  TIMEOUT INCONSISTENCY: Session timeout "varies by classification" but specific timeouts not defined here or in Access Control Policy.

Incident Response Policy

- Classification level determines incident severity assessment
- Data breach notification requirements based on affected classification
- Recovery priorities consider data classification impact

Data Retention Policy

- Retention periods may vary by classification level
- Secure disposal requirements aligned with classification controls
- Legal hold procedures consider classification requirements

  POLICY DEPENDENCY: Multiple dependencies on other policies that are themselves under review or contain conflicting requirements.

Training and Awareness

Initial Training

- All personnel complete data classification training during onboarding
- Role-specific training for Data Owners and Custodians
- Annual refresher training for all staff
- Specialised training for handling RESTRICTED information

Ongoing Awareness

- Quarterly reminders about classification requirements
- Case studies of classification violations and lessons learned
- Regular updates on regulatory changes affecting classification
- Recognition program for exemplary classification compliance

> **TRAINING TRACKING:** No system specified for tracking training completion or measuring effectiveness of training programs.

Review and Updates

This policy will be reviewed annually or when: - Regulatory requirements change - Business model or client base significantly changes
- Major security incidents involving classified information - Technology changes affect classification controls

> **REVIEW TRIGGERS:** Review triggers are appropriate but no specific timeline or process defined for conducting reviews.

Policy updates require approval from: - Data Protection Officer (technical changes) - Legal team (regulatory compliance changes) - Chief Information Officer (significant control changes)
- Board approval (policy framework changes)

> **APPROVAL HIERARCHY:** Complex approval process may delay urgent updates needed for regulatory compliance.

> **IMPLEMENTATION STATUS:** This policy is pending final approval and implementation. Current data handling practices may not fully align with classification requirements. A comprehensive gap analysis and implementation plan is required before enforcement.

KNOWN ISSUES: - Inconsistent terminology and requirements across related policies - Missing technical implementation details and system specifications - Unclear roles and responsibilities with conflicting authority assignments - Incomplete integration with existing security and access control systems - Training and compliance monitoring systems not fully defined

RISK ASSESSMENT: Current draft status creates uncertainty about data handling requirements and may impact regulatory compliance obligations. Prioritise completion and approval to address governance and compliance gaps.