Data Classification and Protection Policy

Organization: AegisCISO
Document ID: POL-DATA-001
Version: 1.0
Effective Date: January 2026
Classification: Internal
Owner: Chief Information Security Officer (CISO)

1. Purpose

This policy establishes the framework for classifying and protecting AegisCISO information assets based on their sensitivity and criticality to ensure appropriate security controls are applied.

2. Scope

This policy applies to:

- All information created, received, or maintained by AegisCISO
- All formats (electronic, paper, verbal)
- All storage locations (on-premises, cloud, mobile)
- All personnel handling AegisCISO data

3. Data Classification Levels

3.1 Classification Scheme

POL-DATA-001-01: Data shall be classified into four levels.

Level	Label	Description
1	Public	Information approved for public release
2	Internal	General business information for internal use
3	Confidential	Sensitive business information requiring prot
4	Restricted	Highly sensitive information with strict acce

3.2 Public Data

POL-DATA-001-02: Public data characteristics.

Definition: Information explicitly approved for public release with no adverse impact from disclosure.

Examples:

- Published marketing materials
- Public website content
- Press releases
- Published annual reports
- Job postings

Handling Requirements:

- No special protection required
- Integrity controls recommended
- Approval required before release

3.3 Internal Data

POL-DATA-001-03: Internal data characteristics.

Definition: General business information intended for internal use only that could cause minor impact if disclosed.

Examples:

- Internal communications
- Organizational charts
- Internal policies and procedures
- Project documentation
- Meeting minutes

Handling Requirements:

- Access limited to employees and authorized contractors
- Basic access controls
- Not shared externally without approval
- Clear desk policy applies

3.4 Confidential Data

POL-DATA-001-04: Confidential data characteristics.

Definition: Sensitive information that could cause significant harm to the organization or individuals if disclosed.

Examples:

- Financial records and forecasts
- Customer information
- Employee personal data (HR records)
- Contracts and legal documents
- Security documentation
- Audit reports
- Strategic plans
- Proprietary business processes

Handling Requirements:

- Access based on need-to-know
- Encryption at rest and in transit
- Logging and monitoring required
- Secure disposal required
- NDA required for third-party access

3.5 Restricted Data

POL-DATA-001-05: Restricted data characteristics.

Definition: Highly sensitive information that could cause severe harm if disclosed, including regulatory penalties.

Examples:

- Authentication credentials
- Encryption keys
- Critical security configurations
- Legal/regulatory investigation data
- Merger and acquisition data
- Board-level strategic decisions
- National security related information
- Medical records (if applicable)

Handling Requirements:

- Strict need-to-know access
- Strong encryption required
- MFA for access
- Enhanced logging and monitoring
- Separate storage/systems where feasible
- Executive approval for access
- Data Loss Prevention (DLP) controls

4. Data Classification Process

4.1 Classification Responsibility

POL-DATA-001-06: Data owners are responsible for classification.

Requirements:

- Data owner assigns initial classification
- Classification based on content and context
- Default to higher classification when uncertain
- Classification reviewed periodically

4.2 Classification Criteria

POL-DATA-001-07: Factors for determining classification.

Consider:

- Legal and regulatory requirements
- Contractual obligations
- Business impact of disclosure
- Reputational impact
- Competitive advantage
- Personal data involved

- Financial sensitivity
- Safety implications

4.3 Reclassification

POL-DATA-001-08: Data reclassification process.

Requirements:

- Reclassify when circumstances change
- Document reclassification reasons
- Update labels and controls
- Notify affected parties

5. Data Labeling

5.1 Labeling Requirements

POL-DATA-001-09: Data shall be labeled with classification.

Format	Labeling Method
Documents	Header/footer on each page
Emails	Subject line prefix [CLASSIFICATION]
Files	Filename suffix or metadata
Databases	Column/field level tagging
Physical	Stamps, stickers, cover sheets
Systems	Banner/watermark

5.2 Label Format

POL-DATA-001-10: Standard classification labels.

Format: AegisCISO - [CLASSIFICATION]

Examples:

- AegisCISO - PUBLIC
- AegisCISO - INTERNAL
- AegisCISO - CONFIDENTIAL
- AegisCISO - RESTRICTED

6. Data Handling Requirements

6.1 Storage Requirements

POL-DATA-001-11: Data storage by classification.

Classification	Storage Requirements
Public	Any approved storage
Internal	Corporate systems, encrypted mobile devices

Confidential	Encrypted storage, approved cloud with DLP
Restricted	Encrypted storage, dedicated systems, geograp

6.2 Transmission Requirements

POL-DATA-001-12: Data transmission by classification.

Classification	Transmission Requirements
Public	Any method
Internal	Corporate email, encrypted channels
Confidential	Encrypted email/channels, secure file transfe
Restricted	End-to-end encryption, dedicated channels, no

6.3 Sharing Requirements

POL-DATA-001-13: Data sharing by classification.

Classification	Internal Sharing	External Sharing
Public	Unrestricted	Unrestricted
Internal	Within organization	With approval
Confidential	Need-to-know	NDA + data owner approval
Restricted	Documented approval	Executive approval + enhanced controls

6.4 Printing Requirements

POL-DATA-001-14: Printing controls by classification.

Classification	Printing Requirements
Public	No restrictions
Internal	Pick up promptly, secure disposal
Confidential	Secure print release, limited copies, secure
Restricted	Secure print with tracking, numbered copies,

6.5 Disposal Requirements

POL-DATA-001-15: Data disposal by classification.

Classification	Electronic Disposal	Physical Disposal
Public	Standard deletion	Recycling
Internal	Secure deletion	Cross-cut shredding
Confidential	Cryptographic erasure or degaussing	Cross-cut shredding, certificate
Restricted	Physical destruction + certificate	Incineration or pulping

7. Data Protection Controls

7.1 Access Controls

POL-DATA-001-16: Access control requirements.

Classification	Authentication	Authorization
Public	None required	None required
Internal	Standard authentication	Role-based
Confidential	Strong authentication	Need-to-know + data owner
Restricted	MFA + additional verification	Executive approval + documented

7.2 Encryption Requirements

POL-DATA-001-17: Encryption requirements by classification.

Classification	At Rest	In Transit
Public	Optional	Optional
Internal	Recommended	Required
Confidential	Required (AES-256)	Required (TLS 1.2+)
Restricted	Required (AES-256)	Required (TLS 1.3, end-to-end)

7.3 Monitoring Requirements

POL-DATA-001-18: Monitoring requirements.

Classification	Access Logging	Monitoring
Public	Optional	Basic
Internal	Recommended	Standard
Confidential	Required	Enhanced + alerting
Restricted	Required + review	Real-time + alerting

8. Special Data Categories

8.1 Personal Data

POL-DATA-001-19: Personal data handling.

Requirements:

- Minimum Confidential classification
- Privacy impact assessment for new processing
- Consent/legal basis documented
- Data subject rights supported
- Retention limits enforced
- Privacy-by-design principles applied

8.2 Financial Data

POL-DATA-001-20: Financial data handling.

Requirements:
- Minimum Confidential classification
- Segregation of duties
- Audit trail maintained
- Regulatory compliance verified

8.3 Health Data

POL-DATA-001-21: Health data handling.

Requirements:
- Restricted classification
- Enhanced encryption
- Access logged and audited
- Regulatory compliance (HIPAA if applicable)

8.4 Authentication Data

POL-DATA-001-22: Authentication data handling.

Requirements:
- Restricted classification
- Stored encrypted/hashed
- Never logged in clear text
- Secure transmission only

9. Data Lifecycle Management

9.1 Data Retention

POL-DATA-001-23: Data retention requirements.

Requirements:
- Retention schedules defined per data type
- Legal/regulatory requirements identified
- Retention enforced technically
- Deletion verified

9.2 Data Archiving

POL-DATA-001-24: Data archiving requirements.

Requirements:
- Archive classification maintained
- Encryption maintained in archives
- Access controls preserved
- Retrieval procedures documented

10. Data Loss Prevention

10.1 DLP Controls

POL-DATA-001-25: Data loss prevention implementation.

Requirements:

- DLP solution deployed for Confidential and Restricted data
- Content inspection enabled
- Policy violations logged and alerted
- Blocking for Restricted data exfiltration
- Regular policy tuning

11. Compliance

11.1 Regulatory Alignment

This policy supports:

- NCA Essential Cybersecurity Controls (ECC-1: 2-5)
- PDPL (Saudi Data Protection Law)
- ISO/IEC 27001:2022 - A.8 Asset Management
- GDPR (if applicable)

12. Roles and Responsibilities

Data Owners

- Classify their data
- Approve access requests
- Review classifications periodically
- Ensure compliance with handling requirements

Data Custodians

- Implement technical controls
- Maintain data protection measures
- Report incidents
- Support data owner decisions

All Users

- Handle data per classification
- Report misclassification
- Report incidents
- Complete data handling training

CISO

- Policy ownership
- Classification framework governance

- Compliance monitoring
- Exception approval

13. Enforcement

Mishandling of classified data may result in:

- Access revocation
- Disciplinary action
- Legal action for intentional breaches
- Regulatory penalties

14. Review

Annual review for:

- New data types
- Regulatory changes
- Incident lessons learned
- Technology changes

15. References

- NCA Essential Cybersecurity Controls
- ISO/IEC 27001:2022
- NIST SP 800-60 (Data Classification)
- Saudi PDPL

Document Control:

Version	Date	Author	Changes
1.0	January 2026	CISO	Initial Release