**Data Classification Policy (DCP)**

**Policy ID:** SEC-DCP-001  
**Version:** 1.0  
**Approval Date:** [Insert Date]  
**Next Review Date:** [Insert Date + 12 months]  
**Owner:** Chief Information Security Officer (CISO)  
**Applies To:** All employees, contractors, vendors, and authorized third-party users who create, access, store, or manage [COMPANY NAME] data

**1. Purpose**

This policy defines how [COMPANY NAME] classifies and handles its information assets based on sensitivity, regulatory requirements, and business impact. Proper classification supports appropriate access controls, risk management, and regulatory compliance.

**2. Scope**

Applies to all organizational data, including digital, printed, and verbal information, stored or processed in any format or location. This includes:

* Structured and unstructured data
* On-premises and cloud-based environments
* Portable media and removable storage
* Emails, reports, records, and internal communications

**3. Policy Statements**

**3.1 Classification Levels**

* All data must be assigned one of the following classifications: Public, Internal Use, Confidential, or Restricted. *(NIST MP-3; ISO 27001 A.5.12)*
* Classifications must be based on regulatory sensitivity, business impact, and contractual obligations. *(NIST PL-2; ISO 27001 A.5.12)*

**3.2 Labeling and Handling**

* Data classified as Confidential or Restricted must be clearly labeled and handled in accordance with secure handling standards. *(NIST MP-3, MP-5; ISO 27001 A.5.13)*
* Printed materials must be labeled accordingly and stored in secured locations. *(NIST PE-3; ISO 27001 A.7.1)*
* Electronic files must include classification markings in file names, metadata, or headers. *(NIST MP-2; ISO 27001 A.5.13)*

**3.3 Storage and Transmission**

* Restricted data must be encrypted in transit and at rest using approved cryptographic methods. *(NIST SC-12, SC-13; ISO 27001 A.8.24, A.8.25)*
* Confidential or Restricted data may not be stored on unauthorized cloud services or personal devices. *(NIST MP-6; ISO 27001 A.5.14)*

**3.4 Access and Disclosure**

* Access to classified data must follow the principle of least privilege and be approved by the designated data owner. *(NIST AC-6; ISO 27001 A.5.18)*
* Sharing of Confidential or Restricted data outside the company requires approval and a data-sharing agreement or NDA. *(NIST AC-20; ISO 27001 A.5.13)*

**3.5 Retention and Disposal**

* Data must be retained only as long as necessary for business or regulatory requirements. *(NIST DM-2; ISO 27001 A.8.10)*
* Expired or unneeded data must be securely deleted or destroyed based on its classification level. *(NIST MP-6; ISO 27001 A.8.11)*

**4. Roles and Responsibilities**

|  |  |
| --- | --- |
| All Users | Understand classification levels; apply labels; protect and handle data properly |
| Data Owners | Determine data classification; approve access; enforce retention requirements |
| IT/Security Team | Enforce technical controls for storage, transmission, and deletion |
| Compliance/Legal | Ensure alignment with legal, contractual, and regulatory requirements |

**5. Compliance and Enforcement**

Noncompliance may result in data leakage, legal penalties, and disciplinary action. [COMPANY NAME] reserves the right to monitor data handling practices and enforce appropriate corrective measures.

**6. Review and Maintenance**

This policy shall be reviewed annually or following significant changes to data protection regulations, information systems, or business requirements. The CISO is responsible for policy updates.

**7. Acknowledgment and Agreement**

I acknowledge that I have read, understand, and agree to comply with [COMPANY NAME]’s Data Classification Policy. I understand that failure to comply may result in disciplinary action or legal consequences.

|  |  |  |
| --- | --- | --- |
| **Name (Print):**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Manager/HR (Print):**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |