Data Classification and Handling

Classification Levels

Public: Information intended for public disclosure. No confidentiality required.

Internal: Information for internal use. Not for public disclosure but low risk if exposed.

Confidential: Sensitive business information. Unauthorized disclosure could harm company.

Restricted: Highly sensitive data. Unauthorized disclosure could cause severe harm. Includes personal data, financial data, trade secrets.

Classification Criteria

Consider: Sensitivity, regulatory requirements, business impact of disclosure, privacy implications.

When in doubt, classify at higher level. Data owner determines classification. Review classification periodically.

Handling Requirements - Public

No special handling required. Can be shared freely. Store on any company system.

Examples: Marketing materials, press releases, public website content, published reports.

Handling Requirements - Internal

Share only with employees and authorized contractors. Don't share on public websites or social media.

Store on company systems with access controls. Email to company addresses only.

Examples: Internal policies, org charts, project plans, internal communications.

Handling Requirements - Confidential

Share only with employees who need to know. Require NDA for external sharing.

Encrypt in transit and at rest. Store on approved systems with strong access controls. Don't store on personal devices.

Examples: Financial results (pre-release), customer lists, contracts, strategic plans, employee data.

Handling Requirements - Restricted

Strict need-to-know access. Require executive approval for external sharing.

Strong encryption required. Multi-factor authentication for access. Detailed access logging and monitoring.

Examples: Customer personal data, payment card data, trade secrets, M&A; information, security vulnerabilities.

Data Labeling

Label documents and emails with classification level. Use classification markings in headers/footers.

Email subject lines should indicate classification for Confidential and Restricted data.

Data Storage

Public/Internal: Standard company storage systems.

Confidential: Encrypted storage with access controls. Approved cloud storage with encryption.

Restricted: Encrypted storage with strict access controls. May require on-premises storage for some data types.

Data Transmission

Public/Internal: Standard email and file sharing.

Confidential: Encrypted email or secure file sharing. VPN for remote access.

Restricted: Encrypted email with additional authentication. Secure file transfer protocols. No transmission to personal email.

Data Disposal

Public/Internal: Standard deletion.

Confidential: Secure deletion ensuring data cannot be recovered.

Restricted: Cryptographic erasure or physical destruction. Certificate of destruction for physical media.

Third-Party Data Sharing

Assess third-party security before sharing Confidential or Restricted data. Require data protection agreement (DPA).

Specify permitted uses, security requirements, and data retention. Audit third-party compliance.

Data Classification Training

All employees complete annual data classification training. Understand classification levels and handling requirements.

Data owners receive additional training on classification decisions. Regular reminders and updates.

Compliance and Audits

Audit data handling practices regularly. Verify compliance with classification requirements.

Report violations to security team. Remediate issues promptly. Track metrics on classification compliance.