

Data Classification Policy

Purpose

Not all information at Your Organization carries the same sensitivity or protection obligations. This policy establishes a consistent classification scheme so that workforce members can recognize what data they are handling, apply proportionate protections, and comply with legal, regulatory, and contractual obligations governing that data.

Scope

This policy applies to all information created, received, stored, processed, or transmitted by Your Organization, in any form (electronic, paper, verbal), regardless of location (on-premises, cloud, endpoint, mobile, removable media, third-party service). It applies to all workforce members and any third party that handles Your Organization information.

Classification levels

Public

Information that has been explicitly approved for public release.

- **Examples.** Published marketing content, press releases, public website pages, published product documentation.
- **Handling.** No special handling required. Integrity remains important — only authorized owners may publish or amend Public information.

Internal

Default classification for day-to-day business information that is not for public distribution but carries no significant harm if disclosed.

- **Examples.** Internal org charts, meeting notes, non-sensitive project plans, internal communications.
- **Handling.** Restrict to workforce members and authorized third parties on a need-to-know basis. Store on Your Organization-approved systems. Do not post on public forums.

Confidential

Information whose unauthorized disclosure could cause meaningful harm to Your Organization, its customers, its partners, or its workforce.

- **Examples.** Customer lists, unreleased financial results, source code, product roadmaps, contracts, HR records, vendor assessments, internal security findings.

- **Handling.** Access on a strict need-to-know basis. Encrypt in transit (TLS 1.2+) and at rest. Do not store on unmanaged endpoints or personal cloud storage. Sharing with external parties requires an NDA and a documented business need.

Restricted

Information subject to the strongest handling requirements, typically because legal, regulatory, or contractual obligations impose specific protections, or because disclosure could cause severe harm.

- **Examples.** Payment card data (PCI), Protected Health Information (PHI/HIPAA), government-regulated data (CUI), personally identifiable information (PII) in bulk, authentication secrets, cryptographic keys.
- **Handling.** Access is limited to the smallest set of users who must have it to perform their duties; access requires documented approval and is reviewed at least quarterly. Must be encrypted in transit and at rest with keys managed in an approved KMS. Must not be copied to endpoints or personal devices. Any access, export, or transmission is logged.

Responsibilities

- **Data Owner.** Accountable for classifying a given data asset, authorizing access, and reviewing classification periodically.
- **Data Custodian.** Implements the controls that protect the data in accordance with its classification (infrastructure team for cloud storage, DBAs for databases, etc.).
- **Workforce members.** Must classify information they create, label it appropriately where reasonable, and handle it per the rules for its classification.

Labeling

Where the system supports it (document management, email, collaboration tools), Confidential and Restricted information must be labeled. Absence of a label does not override classification obligations — the default is Internal.

Transmission

Confidential and Restricted information must be transmitted using Your Organization-approved, encrypted channels. Do not send Confidential or Restricted data over unencrypted email, personal messaging apps, or consumer file-sharing services.

Retention and disposal

Data must be retained only as long as required by the Data Retention Policy and applicable law. Restricted and Confidential data must be disposed of via secure wipe (electronic) or cross-cut shredding (paper). Certificates of destruction must be retained for bulk disposal of Restricted data.

Third parties

Before sharing Confidential or Restricted data with a third party, the relationship must be governed by a written contract with appropriate data protection terms (DPA, BAA, or equivalent) and must be logged in the vendor

inventory.

Scope exceptions

Exceptions must be requested in writing, describe the business need and compensating controls, and be approved by the CISO or designee.

Review cadence

This policy is reviewed annually by the Data Protection Officer (or delegate) and the Information Security team.

Effective date: [the date this policy takes effect]