

Media Protection Policy

Purpose

Sensitive data does not stop being sensitive when it leaves a live production system — it lives on backup tapes, removable drives, decommissioned hard disks, printed reports, and portable storage. This policy defines how Your Organization protects both digital and physical media throughout their lifecycle: access, marking, storage, transport, and sanitization or destruction at end of life.

Scope

This policy applies to all media that stores Your Organization or customer data, including hard disks, solid-state drives, USB and other removable storage, backup media, mobile device storage, and printed or handwritten materials containing Confidential or Restricted information (per the Data Classification Policy). It applies to all workforce members and any third party handling Your Organization media.

Media access

- Access to media containing Confidential or Restricted data is restricted to individuals with a documented business need, consistent with the Access Control Policy.
- Physical media is stored in locked, access-controlled locations (server rooms, locked cabinets, or offsite secure storage facilities) when not in active use.
- Shared or removable media used with multiple systems is subject to the same handling rules as the highest classification level of data it has ever held, until formally sanitized.

Media marking

Physical and removable media containing Confidential or Restricted data is labeled with its classification level so that handlers can apply the correct protections without inspecting content. Unmarked media defaults to Internal handling requirements at minimum.

Removable and portable media

- Use of removable media (USB drives, external disks, memory cards) to store or transport Confidential or Restricted data requires encryption using an Your Organization-approved method.
- Personally owned removable media must not be used to store or transport company or customer data.
- Data loss prevention controls, where deployed, restrict or log the transfer of Confidential and Restricted data to removable media.

Media transport

Media transported outside a controlled facility (courier, mail, in-person transfer) must be encrypted, and its movement logged including sender, recipient, contents description, and date. Accountable personnel are designated for custody of media in transit.

Backup media

Backup media is encrypted, access-restricted, and subject to the same retention and disposal rules as the production data it backs up, per the Data Retention Policy and the Business Continuity and Disaster Recovery Policy.

Sanitization and disposal

- Media reaching end of life is sanitized or destroyed using a method appropriate to its classification before reuse, transfer, or disposal — degaussing, cryptographic erasure, or physical destruction for Restricted data; secure wipe consistent with NIST SP 800-88 guidance for Confidential and Internal data.
- Destruction of media holding Restricted data is documented with a certificate of destruction, retained per the Data Retention Policy.
- Third-party media destruction vendors must be contractually bound to appropriate handling and destruction standards and are assessed per the Vendor Risk Management Policy.

Roles and responsibilities

- **IT Operations.** Executes media sanitization and destruction, and maintains destruction records.
- **Data and System Owners.** Ensure media associated with their systems is inventoried, marked, and disposed of per this policy.
- **Workforce members.** Follow marking and handling requirements for media they use in the course of their work.

Review cadence

This policy is reviewed annually by Information Security and IT Operations, or sooner following a material change in storage technology or a media-handling incident.

Effective date: [the date this policy takes effect]