Data Handling & Classification Guide

Not all data is created equal. Properly classifying and handling data ensures sensitive information receives appropriate protection while enabling efficient collaboration on non-sensitive materials. Mishandling data can result in breaches, regulatory fines, and reputational damage.

Key Points

- ✓ Classify data into levels: Public, Internal, Confidential, Restricted
- ✓ Restricted data (PII, financial, health records) requires encryption at rest and in transit
- ✓ Never send Confidential or Restricted data via unencrypted email
- ✓ Use approved file-sharing platforms — not personal cloud storage or USB drives
- ✓ Apply the "need to know" principle — share only with authorized individuals
- ✓ Label documents with their classification level in headers or footers
- ✓ Follow data retention policies — delete data when it is no longer needed

Action Items

1. Review files on your desktop and classify them appropriately
2. Move any Confidential files from personal cloud storage to approved platforms
3. Enable encryption on your laptop's hard drive (BitLocker / FileVault)
4. Learn your organization's data retention schedule and purge expired data
5. Verify you are using approved tools for sharing sensitive documents

Quick Reference

Classification Levels:
Public — Marketing materials, press releases (no restriction)
Internal — Policies, org charts (employees only)
Confidential — Financial reports, strategic plans (authorized teams only)
Restricted — PII, health data, credentials (strict access controls, encrypted)