CSNP
CYBERSECURITY NON-PROFIT

Data Classification Guide

A comprehensive framework for protecting your organization's most valuable asset: information. Learn how to implement effective data classification to strengthen security, ensure compliance, and reduce risk.

CYBERSECURITY NON-PROFIT

CSNP

Why Data Classification Matters

Protect What Matters

Not all data requires the same level of protection. Classification helps you allocate resources effectively and secure your most sensitive information.

Ensure Compliance

Meet regulatory requirements like GDPR, HIPAA, and industry standards by demonstrating proper data handling and protection measures.

Reduce Risk

Minimize the impact of data breaches by controlling access, implementing proper safeguards, and knowing exactly what you're protecting.

Enable Efficiency

Clear classification streamlines workflows, reduces confusion, and ensures employees handle data appropriately without constant oversight.

Four Levels of Data Classification

Understanding these levels is the foundation of your data protection strategy. Each level requires different handling procedures and security controls.

Public

Information intended for public consumption with no restrictions. Disclosure causes no harm to the organization.

Internal

Information for internal use only. Unauthorized disclosure could cause minor inconvenience but not significant harm.

Confidential

Sensitive business information. Unauthorized disclosure could cause significant harm, financial loss, or competitive disadvantage.

Restricted

Highly sensitive information requiring the highest protection. Unauthorized disclosure could cause severe damage, legal liability, or catastrophic harm.

Data Type Examples by Classification Level

Public

- Press releases
- Marketing materials
- Job postings
- Published reports
- Website content

Internal

- Employee directory
- Internal memos
- Meeting notes
- Org charts
- Training materials

Confidential

- Financial records
- Customer lists
- Business plans
- Vendor contracts
- Product roadmaps

Restricted

- Social Security numbers
- Payment card data
- Medical records
- Passwords
- Legal documents

Labeling Requirements

Clear, consistent labeling ensures everyone understands how to handle data appropriately. Implement these standards across all formats.

01

Document Headers & Footers

Add classification labels to the top and bottom of every page in documents, presentations, and reports.

02

Email Subject Lines

Include classification in brackets at the beginning of email subjects: [CONFIDENTIAL] Budget Review Meeting.

03

File Names & Metadata

Incorporate classification into file names and use metadata tags for easy identification and sorting.

04

Physical Documents

Use colored stamps, labels, or cover sheets on printed materials to indicate classification level.

Handling Procedures by Classification Level

Public

Access: Unrestricted

Sharing: No approval needed

Disposal: Standard recycling

Internal

Access: All employees

Sharing: Within organization only

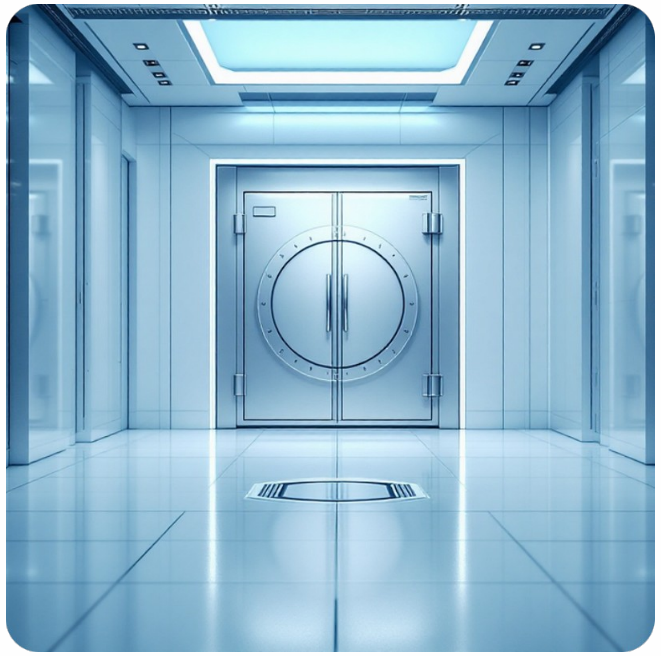
Disposal: Secure deletion

Confidential

Access: Need-to-know basis

Sharing: Manager approval required

Disposal: Shred or secure wipe



Restricted

Access: Specific authorization

Sharing: Executive approval, NDAs

Disposal: Certified destruction

Storage & Transmission Requirements

Storage Requirements

Public & Internal

- Standard file servers
- Cloud storage allowed
- Regular backups

Confidential

- Access-controlled systems
- Encryption at rest
- Audit logging enabled

Restricted

- Highly secure systems
- Strong encryption
- Multi-factor authentication

Transmission Rules

Public & Internal

- Standard email acceptable
- No encryption required
- Internal networks ok

Confidential

- Encrypted email required
- Secure file transfer
- VPN for remote access

Restricted

- Approved channels only
- End-to-end encryption
- Documented transfers

Data Classification Policy Template

Use this framework to develop your organization's formal data classification policy. Customize to meet your specific needs and regulatory requirements.

1

Purpose & Scope

Define why classification is needed and what data/systems are covered by the policy.

2

Classification Levels

Document your four levels with clear definitions and examples for each category.

3

Roles & Responsibilities

Assign ownership: who classifies data, who approves access, who monitors compliance.

4

Handling Procedures

Specify requirements for storage, transmission, access, and disposal at each level.

5

Compliance & Review

Establish audit processes, violation consequences, and annual policy review schedule.

Implementation Checklist

Getting Started

- **Conduct data inventory**

  Identify all data types and locations across your organization

- **Develop policy document**

  Create formal policy using the template framework

- **Classify existing data**

  Apply classification levels to current data assets

- **Train all employees**

  Ensure everyone understands their responsibilities

Maintaining the Program

- **Implement technical controls**

  Deploy encryption, access controls, and monitoring tools

- **Label all new data**

  Make classification part of document creation workflow

- **Monitor compliance**

  Regular audits and spot checks to ensure adherence

- **Review and update**

  Annual policy review and continuous improvement

About Cybersecurity Non-Profit

Making cybersecurity knowledge accessible to everyone through education, community, and practical resources.

Business & Non-Profit Security

Family Cybersecurity

Kids Safety

Senior Digital Safety

Women's Security

Parents & Educators

Everything we offer is free. Visit us at **csnp.org** to learn more and access our comprehensive resource library at **csnp.org/resources**