CSNP
CYBERSECURITY NON-PROFIT

Data Protection Training

Essential training for protecting personal and confidential data in your organization

CSNP TRAINING SERIES

What is Personal Data?

Direct Identifiers

Names, addresses, social security numbers, email addresses, phone numbers, and government-issued ID numbers

Sensitive Information

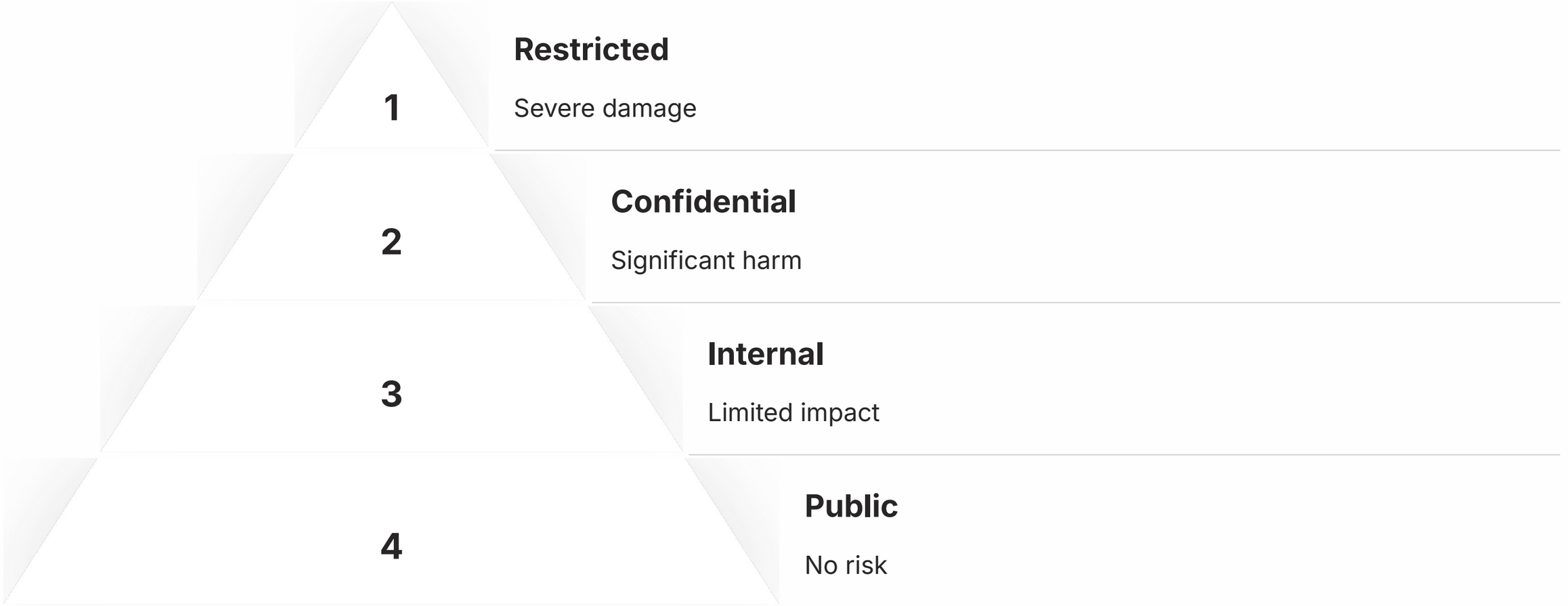
Financial records, health data, biometric data, and any information about race, religion, or political beliefs

Digital Identifiers

IP addresses, device IDs, cookies, location data, and online behavioral information

Personal data is any information that can identify an individual, either directly or when combined with other data. Understanding what constitutes personal data is the first step in protecting it.

Data Classification System



Not all data requires the same level of protection. Our classification system helps you determine appropriate security measures based on sensitivity and potential impact of unauthorized disclosure.

Handling Confidential Data

01

Verify Need-to-Know

Only access confidential data when required for your job responsibilities

02

Use Secure Methods

Access through encrypted connections and approved company systems only

03

Protect During Use

Lock screens when away, avoid public viewing, use privacy filters

04

Secure After Use

Log out properly, return documents to secure storage, clear sensitive data

Data Storage Requirements

Digital Storage

- Store sensitive data only on approved company systems
- Enable encryption for all devices containing confidential information
- Use strong passwords and enable multi-factor authentication
- Avoid storing work data on personal devices or cloud services

Physical Storage

- Keep confidential documents in locked cabinets or rooms
- Restrict access to authorized personnel only
- Maintain access logs for restricted areas
- Never leave sensitive documents unattended in open areas

Data Transmission Security

Email Encryption

Use encrypted email for sensitive data. Never send passwords or financial information via unencrypted email

Approved Platforms

Only use company-approved file sharing and collaboration tools with proper security controls

Verify Recipients

Double-check email addresses and confirm recipient identity before sending confidential information

Email and File Sharing Best Practices

Check Before Sending

Review recipient list, subject line, and attachments. Remove unnecessary recipients from sensitive communications.

Use Secure Attachments

Password-protect sensitive documents. Send passwords through separate communication channels.

Be Cautious with Links

Use official file-sharing platforms. Set expiration dates and download limits for shared files.

Watch for Phishing

Verify unexpected requests for data. Never click suspicious links or download unknown attachments.

Physical Document Security

Clean Desk Policy

Maintain a clean desk by securing all confidential documents when not in use, even for short breaks.

Printing Precautions

- Retrieve printed documents immediately from printers
- Use secure printing features when available
- Shred sensitive documents rather than discarding in trash

Visitor Awareness

Be mindful of visitors and contractors. Secure documents before meetings in shared spaces.

Data Retention and Disposal

Retention Requirements

Follow company policies and legal requirements for how long to keep different types of data

Secure Disposal

Use approved methods: shredding for paper, certified data wiping for digital media

1

2

Regular Review

Periodically review stored data and identify information that has reached end of retention period

3

4

Documentation

Maintain records of data disposal activities for compliance and audit purposes

Important: Never dispose of confidential data in regular trash or recycling. Always use designated secure disposal methods.

Privacy Regulations Overview

GDPR (EU)

General Data Protection Regulation applies to EU residents' data. Requires consent, data minimization, and breach notification within 72 hours.

CCPA (California)

California Consumer Privacy Act gives residents rights to know, delete, and opt-out of data sales. Applies to businesses meeting size thresholds.

Industry Standards

Additional requirements may apply: HIPAA for healthcare, PCI-DSS for payment cards, FERPA for education records.

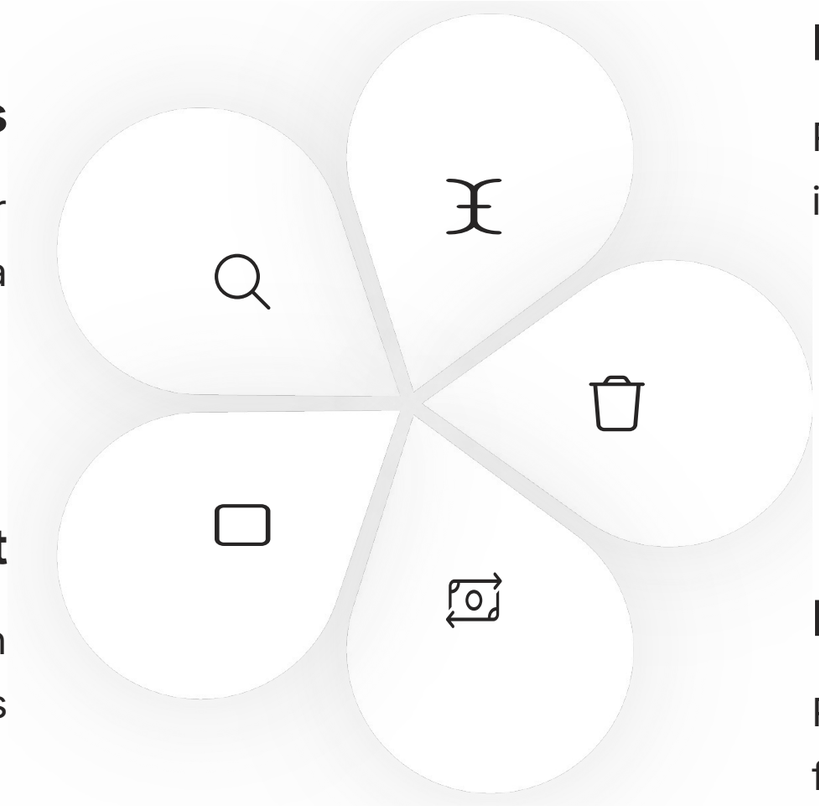
Data Subject Rights

Right to Access

Individuals can request copies of their personal data

Right to Object

Object to processing for certain purposes



Right to Rectification

Request correction of inaccurate information

Right to Erasure

Request deletion of data when no longer needed

Right to Portability

Receive data in machine-readable format

Understanding these rights helps you respond appropriately to data subject requests and maintain compliance with privacy regulations.

Data Breach Response Protocol

Immediate Action

Stop the breach if possible. Disconnect affected systems. Do not delete evidence.

Report Quickly

Notify your manager and IT security team immediately. Time is critical for breach response.

Contain & Assess

Security team isolates affected systems and determines scope of compromised data.

Notify & Remediate

Legal team handles required notifications. Organization implements fixes to prevent recurrence.

Critical: Report suspected breaches within 1 hour of discovery. Early reporting can significantly reduce damage and regulatory penalties.

Knowledge Check

Question 1

Which of these is NOT considered personal data?

A) Employee ID number
B) Company revenue figures
C) Email address
D) IP address

Question 2

How should you send a confidential document via email?

A) Regular email is fine
B) Encrypted email with password
C) Personal email account
D) Text message attachment

Question 3

What should you do if you suspect a data breach?

A) Investigate yourself first
B) Delete all evidence
C) Report to IT immediately
D) Wait until you're certain

Answers: 1-B, 2-B, 3-C

Key Takeaways

- **Classify Before You Act**

  Understand data sensitivity and apply appropriate protections

- **Security is Everyone's Job**

  Your actions directly impact organizational data security

- **Think Before You Click**

  Verify recipients, use encryption, follow secure practices

- **When in Doubt, Ask**

  Contact IT security if you're unsure about proper procedures

- **Report Immediately**

  Quick breach reporting minimizes damage and ensures compliance

About CSNP

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

Our Programs

Business & Non-Profit Security

Family Cybersecurity

Kids Safety

Senior Digital Safety

Women's Security

Parents & Educators

Everything we offer is completely free. Visit **csnp.org** to learn more or access training resources at **csnp.org/resources**