Published on *University of Colorado* (https://www.cu.edu)

Data Classification [1]

Sensitive university information must be protected from compromise, such as unauthorized or accidental access, use, modification, destruction, or disclosure. Classifying or labeling the information helps determine the minimum security requirements necessary to keep it safe.

The university has adopted the following data classification types:

- Highly Confidential Information
- Confidential Information
- Public Information

The type of classification assigned to information is determined by the Data Trustee—the person accountable for managing and protecting the information's integrity and usefulness.

Review the Data Classification Table for the types of information you access, handle, or store. (Be mindful this is not an exhaustive list of examples.)

IMPORTANT: Regulated data such as **HIPAA** and **Payment Card Industry (PCI)** may have additional security requirements. If you access, handle, or store such data, contact your campus-specific IT department for more information.

In order to fully understand the risk associated with a service, make sure to take into account both the data classification and impact.

Learn more about Adverse Impact [2]

Data Classification Table

Type	Description	Examples

Highly Confidential

This type includes data elements that require protection under laws, regulations, contracts, relevant legal agreements and/or require the university to provide notification of unauthorized disclosure/security incidents to affected individuals, government agencies or media.

Requirements when accessing, handling or storing:

- When possible, use university-supported services or systems that have been approved for handling highly confidential data.
- Only share with the people who need to know it for an authorized use, includes verbal and written information.
- Encrypt the information when transmitting or storing.
- Ensure networks or systems used to handle or store the information have appropriate firewalls, monitoring, logging, patching, anti-malware and related security controls.
- Use university-provided computers, including mobile computing devices and storage medium. If this is not possible and you must use a personal computer, for example when working remotely, use remote desktop to connect to your university-provided computer.
- Document the policy for data retention.
- Contact your campus's information security office to ensure protection of data if compensating controls are used to secure the data in place of the above mentioned controls.

- Protected health information
- Social security numbers
- Payment card numbers
- Financial account numbers: including university account numbers, student account numbers, and faculty and staff direct deposit account numbers
- Driver's license numbers
- Health insurance policy ID numbers
- Level 4 and 5 of Student Data (SSN, NID, Financial Aid (except work study), loan and bank account numbers, health information, disability, race, ethnicity, citizenship, legal presence, visas, religion, sexual orientation, sex at birth)
- Grievances/disciplinary actions
- Research, proposals, research plans, and results subject to International Traffic in Arms Regulations/Export Administration Regulations (ITAR/EAR)
- Controlled Unclassified Information (CUI)

Confidential	This type includes data elements usually not disclosed to the public but are less sensitive than Highly Confidential data. If a legally required and applicable Colorado Open Records Act (CORA) request is submitted, these records may be released. **Requirements when accessing, handling or storing:** • Only share with the people who need to know it for an authorized use, includes verbal and written information. • Encrypt the information when transmitting or storing. • Ensure networks or systems used to handle or store the information has appropriate firewalls, monitoring, logging, patching, anti-malware and related security controls. • Use university-provided computers, including mobile computing devices and storage medium. If this is not possible and you must use a personal computer, for example when working remotely, use remote desktop to connect to your university-provided computer.	• Faculty and staff personnel records, benefits, salaries, performance evaluations, and employment applications • Admission applications • University insurance records • Donor contact information and non-public gift amounts • Fundraising information • Non-public policies • Internal memos and email, and non-public reports • Purchase requisitions, cash records, budgetary plans • Non-public contracts • University and employee ID numbers • Level 2 and 3 of Student Data (Military status, veteran's status, GPA, course grades, probation, suspension, COF, service indicators, all non-directory data not listed, work study information, gender, gender identity, pronoun, birth date, dorm, emergency info, student ID, UUID, residency) • Research proposals • Research plans and results • Instructional materials • Internal/unpublished business documents
Public	This type includes any information on university websites to which the data owner allows access without authentication and information made freely available through university print material.	• Directory data • Public policies • Published business documents

Groups audience:
Office of Information Security
Right Sidebar:
security data classification resources

Source URL: https://www.cu.edu/security/data-classification

Links
[1] https://www.cu.edu/security/data-classification

[2] https://www.cu.edu/security/about-adverse-impact