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

Data Classification [1]

Sensitive university data must be protected from compromise, such as unauthorized or accidental access, use, modification, destruction or disclosure.

Classifying or labeling the data helps determine the minimum-security requirements necessary to keep it safe.

The University of Colorado 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 data you access, handle or store. (Be mindful this is not an exhaustive list of examples.)

IMPORTANT: Regulated data, such as **HIPAA** and the **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.

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

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 are authorized to use it for legitimate business purposes; this includes verbal and written information.
- Encrypt the data when sending or storing.
- Ensure networks or systems used to handle or store the data have appropriate firewalls, monitoring, logging, patching, anti-malware, and related security controls.
- Use university-provided computers when accessing or processing data. If this is not possible and you must use a personal computer, use a remote desktop to connect to your university-provided computer.
- Document the policy for data retention.
- Contact your campus 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 data
- Social Security numbers
- Payment card numbers
- Financial account numbers including university account numbers, student account numbers and faculty and staff direct deposit numbers
- Driver's license numbers
- Levels 4 and 5 of student data (See Use Guidelines for Student Data [2])
- Grievances/disciplinary action records
- Research, proposals, research plans and results to International Traffic in Arms Regulations/Export Administration Regulation (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 are authorized to use it for a legitimate business purpose. This includes verbal and written information. • Ensure networks or systems used to handle or store the data have appropriate firewalls, monitoring, logging, patching, anti-malware, and related security controls. • Use university provided computers when accessing or processing data. If this is not possible and you must use a personal computer, use a remote desktop to connect to your university-provided computer.	• Faculty and staff personnel records, benefits, salaries, performance evalautions and employment applications • University insurance records • Donor contact data and non-public gift amounts • Fundraising data • Non-public policies • Internal memos and emails, and non-public reports • Purchase requisitions, cashg records, budgetary plans • Non-public contacts • University and employee ID numbers • Levels 2 and 3 of student data (See Use Guidelines for Student Data [2]) • Research proposals • Research plans and results • Internal/unpublished business documents
Public	This type includes any data on university websites to which the data trustee allows access without authentication and data made freely available through university print material.	• Directory data • Public policies • Published business documents

Other data classifications:

- Employee data use guidelines [3]
- Student data use guidelines [2]

Adverse Impact

Equally important to classification, sensitive university information is also evaluated for the potential adverse impact to CU if the information has a loss of confidentiality, integrity or

availability. The impact levels are high, moderate and low. The Adverse Impact Table below provides descriptions for each level.

The university considers the following when determining the adverse impact level:

- Financial costs, direct or indirect
- Reputational damage
- Safety of community members
- Legal or regulatory compliance action

Adverse Impact Table

Level	Description	Financial	Reputation	Safety	Legal

High	The potential impact is high if the loss of confidentiality, integrity or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, assets or individuals. A severe or catastrophic effect might result in: • Severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions. • Major damage to organizational assets. • Major financial loss. • Severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.	Direct or indirect monetary costs to the university to which liability must be transferred to an organization that is external to the campus, as the university is unable to incur the assessed high end of the cost for the risk.	Negative press coverage and/or major political pressure on the university reputation on a national or international scale.	Places campus community members at imminent risk for injury.	Significant legal and/or regulatory compliance action against the university or business.

Moderate	The potential impact is moderate if the loss of confidentiality, integrity or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect might result in: • Significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the function is significantly reduced. • Significant remediation cost to the university.	Direct or indirect monetary costs to which liability is transferred to the campus as the business unit/school is unable to pay the assessed high-end cost for the risk.	Negative press coverage and/or minor political pressure on university reputation on a local scale.	Noticeably increases likelihood of injury to community members.	Comparatively lower but not insignificant legal and/or regulatory compliance action against the university of business.

Low	The potential impact is loss of confidentiality, integrity or accountability could be expected to have a limited adverse effect on organizational operations, organizational assets or individuals. A limited adverse effect might result in: • Degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the function is noticeably reduced. • Minor damage to organizational assets. • Minor financial loss. • Minor harm to individuals.	Direct or indirect monetary costs to the university to which business unit/school can solely pay the assessed high-end cost for the risk.	Nominal impact and/or negligible political pressure on university reputation on a local scale.	Nominal impact on safety of campus community members.	No or insignificant legal and/or regulatory compliance action against the university or business.

NOTE: The descriptions are provided only as guides and should not be considered without the context of the broader environment. While making the impact determinations, it is important to realize that the value of an information type may change during its life cycle. So, information subtypes may include the relevant statements. For example, consider the case of contracts as an information type. The subtypes could be contracts-initial discussion, contracts-finalized, contracts-terminated and all these subtypes may have different impact levels for the security categories.

Groups audience:
Data Governance

Source URL:https://www.cu.edu/data-governance/resources-support/data-classification

Links
[1] https://www.cu.edu/data-governance/resources-support/data-classification [2] https://www.cu.edu/data-governance/resources-support/data-classification/student-data-use-guidelines [3] https://www.cu.edu/data-governance/resources-support/data-classification/employee-data-use-guidelines