Classify and Comply: Understanding your data is the first step to protecting it [1]

Important to know
Mismanaging highly confidential or confidential data could have a significant adverse impact to CU including financial costs (direct or indirect); reputational damage; jeopardizing the safety of community members; and legal or regulatory compliance action.

Why is data classified?
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 has adopted the following data classification types:

- Highly Confidential Information
- Confidential Information
- Public Information

Information is available in all forms: paper, verbal, and electronic.

What can happen when highly confidential or confidential data is mismanaged?
The possibility of a security incident increases when data is mismanaged, putting the university at significant risk of financial loss, reputational damage, safety of community members, and legal or regulatory compliance action.

Real examples of the consequences of data mismanagement

- A university faculty member attached the wrong file to an email they sent to their class, accidentally revealing the grades for all the students to every member of the class.
- The confidentiality terms of a contract with a granting agency were violated after a researcher improperly shared proprietary data, damaging the reputation of the university and putting US defense secrets at risk.
- An error in a university’s degree auditing software allowed anyone accessing the system to view the names, courses, and grades of the 12,000 students enrolled at the university.
- A state official accidentally emailed confidential data, including the identity of a whistleblower, to the wrong person. The official typed an incorrect character into the email’s TO: field, causing the autofill feature to automatically enter the wrong name and
email address. Unfortunately, the field was not corrected before the email was sent.

- The Veteran’s Administration reported 26.5 million discharged veterans’ records, including name, social security number, and date of birth were stolen from the home of an employee who improperly took the data home.
- A law firm employee received an email and clicked on a link to download a document. The employee was then prompted to enter her login credentials into what she believed was a legitimate website. It later came to the employee’s attention that she was no longer receiving emails and reported it to the IT department. It was discovered that the email account had been compromised by a cybercriminal when the employee entered her login credentials. The cybercriminal was able to respond to several client emails using a spoofed email account, advising them of a change of bank details. This resulted in two clients making significant payments to the cybercriminal.
- A state’s human resources department notified parents of infants born within a two-year period that paper records containing parents’ social security numbers and medical histories were discarded without shredding.

What are examples of highly confidential data?

- Protected health data
- Social Security numbers
- Payment card numbers
- Health insurance policy ID numbers
- Financial account numbers: including university account numbers, student account numbers, and faculty and staff direct deposit account numbers
- Driver’s license numbers
- Level 4 and 5 of student data
- Grievances/disciplinary action records
- Research, proposals, research plans, and results subject to International Traffic in Arms Regulations/Export Administration Regulations (ITAR/EAR)
- Controlled Unclassified Information (CUI)

Be mindful this is not an exhaustive list of examples.

What are examples of confidential data?

- Faculty and staff personnel records, benefits, salaries, ID numbers, and employment applications
- Admission applications
- University insurance records
- Donors’ contact data and non-public gift amounts
- Fundraising data
- Non-public policies
- Internal memos and emails, and non-public reports
- Purchase requisitions, cash records, and budgetary plans
- Non-public contracts
- University and employee ID numbers
- Level 2 and 3 of student data
- Research proposals
- Research plans and results
- Internal/unpublished business documents

Be mindful this is not an exhaustive list of examples.

**What are examples of public data?**

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

**What are the required actions when managing highly confidential or confidential data?**

**Highly confidential data**

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.

- 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 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.

**Confidential data**

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.

- Only share with the people who are authorized to use it for legitimate business purposes; 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 remote desktop to connect to your university-provided computer.

If your job responsibility includes providing IT services, be sure to contact your campus Information Security department with any questions or concerns.

**What about compliance with FERPA, HIPAA, PCI?**

Data subject to FERPA, HIPAA, Payment Card Industry (PCI), and other regulatory frameworks may have additional security requirements. If you access, handle, or store such data, contact your campus IT department or compliance liaison for guidance to ensure appropriate measures are in place.

Visit the Office of Information Security [Resources](https://www.cu.edu/security/resources) webpage for more information.

**How do I report possible data mismanagement?**

If you believe data has been inappropriately handled and an information security incident has occurred, it is important to report it as soon as possible. This allows the investigative team to act quickly to determine the level of impact and contain the incident. It is especially critical that incidents are investigated where we have an obligation to external entities to report: these could include medical data, payment card data, research data, etc.

Visit [Reporting an Incident](https://www.cu.edu/security/reporting-incident) to learn more.

**Questions?**

Contact your campus IT department. See the sidebar "Campus IT Departments" on the webpage.

**Groups audience:**
Office of Information Security

**Right Sidebar:**
Review and Bookmark for Future Reference
Campus IT Departments

**Source URL:** https://www.cu.edu/security/classify-and-comply-understanding-your-data-first-step-protecting-it

**Links**
[2] https://www.cu.edu/security/resources