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

Reporting an Incident [1]

What is an information security incident?

An information security incident is any event that, regardless of accidental or malicious cause, results in the any of the following:

- Disclosure of university information to someone unauthorized to access it
- Unauthorized alteration of university information
- Loss of information that the university is legally or contractually bound to protect or that which supports critical university functions
- Disrupted information technology service
- Violation of the university's information security policies

Examples of a possible incident include:

- Loss or theft of university-issued or personally-owned devices or physical media (e.g., USB drives, hard drives, paper files) storing CU sensitive information
- Suspected virus or malware
- Unauthorized access or changes to systems, software, or sensitive information
- Compromised user account
- Accidental exposure of sensitive information (e.g., misdirected email, paper left on a printer)

Why it's important to report suspected incidents

If you believe 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.

Potential impacts include:

- Loss of reputation, affecting enrollment
- Loss of sensitive data, exposing the campus to fines and lawsuits
- Decrease in grants, donations, and alumni involvement
- Loss of student, faculty, staff, and community trust

Information security incidents can happen to anyone. No retaliation will be taken against anyone who, in good faith, reports a possible information security incident.

Information to include in the incident report

Provide the following information when reporting an incident:

1. Contact information
2. College or department involved
3. Brief description of what happened
4. General description of the type of information involved
    - (Was it sensitive university information? Was it shared with or accessed by unauthorized people?)
5. General description of the impact of the incident, if known
6. Any other known resources affected

If the incident involves a lost or stolen mobile device, include the police report number (see section “What to do if the information security incident involves a lost or stolen device”

Groups audience:
Office of Information Security
Right Sidebar:
ois_incident_contact

Links
[1] https://www.cu.edu/security/reporting-incident