

**REED COLLEGE
COMMUNITY SAFETY
DEPARTMENTAL DIRECTIVE**

COMPUTER THEFT REPORTING

Source: Departmental Directive issued by the CS Director, in collaboration with the Chief Information Officer (CIO).

Original publication: August 2010

Latest review & revision: February 2021

Departmental Policy

All suspected, reported, or confirmed losses of Reed-owned computers shall be immediately reported to the Chief Information Officer and the Director of Community Safety.

Purpose

Due to the potential sensitivity of the information stored on Reed computers, the information compromised through the loss or theft of a computer must always be considered a significant risk until a complete investigation is conducted to determine whether or not an actual data breach has taken place. Because of this, the Reed College Electronic Data Security Incident Response Plan requires immediate notification to the Chief Information Officer (CIO) when a Reed-owned computer is missing. While Community Safety is responsible for the initial field investigation and documentation, the CIO is ultimately responsible for completing an investigation, determining whether or not a data breach has occurred, and initiating any necessary mitigation and follow-up action. Additionally, the Director of Community Safety, or designee, is responsible for collaborating with the CIO on investigations and providing any required support or investigative expertise.

Procedure

Dispatcher Responsibilities

Immediately after receiving a report of a possible or confirmed missing, lost, or stolen computer, the on duty Dispatcher shall take the following steps in the order listed below:

- ❑ Create a CAD event for Theft in the ARMS system and dispatch an officer or supervisor, as appropriate
- ❑ Send an email to tech-theft@reed.edu, cio@reed.edu, and cs-ocmgr@reed.edu (CS Managers) that lists any immediately known information about the computer (e.g., name & contact information of the reporting party, name and contact information of the computer owner (if different), time & date of incident or report, location, etc.)
- ❑ Call the Community Safety Manager On-Call and make a verbal notification (or leave a voicemail), *in addition to* sending an email to the cs-ocmgr@reed.edu

**REED COLLEGE
COMMUNITY SAFETY
DEPARTMENTAL DIRECTIVE**

- ☐ Document in Police Information in the CAD event that the above notifications have been made

Responding Officer Responsibilities

- ☐ Respond as appropriate
- ☐ Use the Lost or Stolen College-Owned Computing Equipment Report (see attached) to conduct an initial investigation
- ☐ Document all other relevant information, including taking photographs, interviewing potential witnesses, collecting evidence (i.e., cut cables), etc.
- ☐ Immediately forward all documented information to tech-theft@reed.edu and cs-ocmgr@reed.edu. This information shall be forwarded as soon as it is collected, and forwarding shall not be delayed until a final report is completed and approved
- ☐ Complete an incident report per departmental procedures

Director or Designee Responsibilities

- ☐ Review the initial report and ensure that Community Safety field staff complete the field investigation and report
- ☐ Review the incident report and forward the final report to the CIO at cio@reed.edu

**REED COLLEGE
COMMUNITY SAFETY
DEPARTMENTAL DIRECTIVE**

Lost or Stolen College-Owned Computing Equipment Report

Date & time equipment reported missing

date time:

Reporting party:

name student/department phone

Equipment owner/custodian (if different from reporting party):

name (or classroom/lab use) department or student phone

Last person known to have seen the equipment (if different from reporting party):

name department or student phone

Last known equipment location:

building room within room location (e.g., on desk, in drawer, etc.)

Last day & time equipment was seen at the above location:

Equipment description:

_____ lab/desktop/other _____ serial no. (supplied by CIS)

_____ lab/desktop/other _____ serial no. (supplied by CIS)

**REED COLLEGE
COMMUNITY SAFETY
DEPARTMENTAL DIRECTIVE**

Confidential data:

Does the reporting party believe that confidential data were contained on the missing equipment? (i.e., social security numbers, birth dates, credit card numbers, financial account numbers, driver's license numbers, health or counseling records, student records, etc.)

Data security:

_____ Does the reporting party believe that the equipment was powered down prior to its disappearance?

_____ Does the reporting party believe that Disk Encryption (FileVault or other) was in use prior to the equipment's disappearance?

_____ Does the reporting party believe that any and all confidential materials were stored in encrypted disk images or encrypted folders?

Data backup:

_____ Does the reporting party believe that data on the missing equipment was backed up online?

_____ Does the reporting party believe that the data on the missing equipment was backed up to an external device?

_____ If data was backed up to an external device, is that device still available?

Equipment security:

_____ room location was secured against unauthorized entry

_____ evidence of forced entry to room

REED COLLEGE
COMMUNITY SAFETY
DEPARTMENTAL DIRECTIVE

_____ security cable was not in use

_____ security cable used but was severed or ripped off

_____ security cable used but was unlocked and present

_____ security cable used but was missing

_____ laptop was in locked file drawer or cabinet

_____ laptop was in unlocked file drawer or cabinet or other location

_____ find-location software was in use on the missing equipment

_____ remote data wipe is active for the missing equipment (iPhone, iPad, etc.)

Other relevant information (e.g., persons with keys to room, security cables, etc.)

Name of Community Safety Officer submitting report:

Date and time report submitted to CIO:

time

date