REED COLLEGE
DEPARTMENT OF COMMUNITY SAFETY
DEPARTMENTAL DIRECTIVE

COMPUTER THEFT REPORTING
(Source: Departmental Directive issued by the CS Director, in collaboration with the Chief Technology Officer (CTO), August 13, 2010

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

Purpose
Due to the potential sensitivity of the information stored on Reed computers, the compromise of information 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 breach has taken place. Because of this, the Reed College Electronic Data Security Incident Response Plan requires immediate notification to the CTO (Chief Technology Officer) when a computer is missing. While Community Safety is responsible for the initial field investigation and documentation, the CTO 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 is responsible for collaborating with the CTO 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 e-mail to cio@reed.edu and to grangerg@reed.edu (CS Director) 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 Chief Technology Officer at 971-221-2497 and make a verbal notification (or leave a voice mail) *in addition to* sending an e-mail
- ☐ Call the Director of Community Safety at (503) 777-7379 and make a verbal notification (or leave a voice mail) *in addition to* sending an e-mail
- ☐ Document in Police Information in the CAD event that the above notifications have been made

Responding Officer Responsibilities
- ☐ Respond as appropriate
- ☐ Used attached Report template 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 cio@reed.edu and grangerg@reed.edu. This information shall be forwarded as soon as it is collected and forwarding shall not be delayed until a final report is complete 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

REED COLLEGE
DEPARTMENT OF COMMUNITY SAFETY
DEPARTMENTAL DIRECTIVE

Lost or Stolen College-Owned Computing Equipment Report

Date & time equipment reported missing _____   _____
                                                          date   *time*

Reporting party:

_____   _____   _____
name   *department or student*   *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.)*

Equipment description:

_____laptop/desktop/other _____ Serial no. *(supplied by CIS)*

_____laptop/desktop/other _____ Serial no. *(supplied by CIS)*

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 (PGP, 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

_____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

_____lo-jack 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 CTO: _____ _____
                                          date   *time*