

SECTION: 1.0 GENERAL

SUBJECT: LOST OR STOLEN IT EQUIPMENT

Title: Lost or Stolen Information Technology Equipment Policy

Background: All college-owned computing devices store various forms of Lewis-Clark State College (LC State) information. Some of that information may be considered protected or confidential based on various Federal or State laws, State Board of Education policies, or college policies, rules, or guidelines. Should the devices become lost or stolen, the college may be required to report the data contained on the device as lost which may comprise a breach.

Point of Contact: Director of Information Technology and LC State Risk Manager

Other LC State offices directly involved with the implementation of this policy, or significantly affected by the policy: All LC State Offices

Date of approval by LC State authority: August xx, 2024

Date of State Board Approval: NA

Date of Most Recent Review: August xx, 2024

Summary of Major Changes incorporated in this revision to the policy: New Policy

1. Philosophy

- A. Loss or theft of a device owned by LC State, regardless of the information stored on the device, creates a risk to college systems. A serious risk is created if the lost or stolen device contains restricted/confidential information about students, faculty, staff, alumni, donors, retirees, contractors, or others with whom LC State does business. Therefore, to protect LC State resources, systems, information, and integrity, this policy guides college employees on reporting lost and stolen equipment.
- B. Devices covered under these rules and procedures include any device that is college or personally owned and contains LC State information. Information includes but is not limited to work, research, documents, or other information relating to work or services done at LC State; information relating to employees; information relating to any LC State grants or contracts; and LC State student information. Examples of devices include desktops, laptops, tablets, USB storage devices, portable hard drives, and smartphones. This process addresses a device that is lost or stolen from the campus premises, as well as from off-campus locations.

2. Definitions

- A. Information
Refers to a body of knowledge or data obtained, produced, organized, shared, or managed throughout its business operations. Information may be shared or stored in a physical or electronic manner. Information is not easily replaced without funding, skill, knowledge, resources, time, or any combination of these factors. Therefore, Information is considered a critical college asset used to build knowledge and sustain and create organizational value.
- B. Information Technology equipment
Includes but is not limited to all workstations, laptops, tablets, USB storage devices, portable hard drives, and smartphones.
- C. Lost device
Refers to a device that has been misplaced and cannot be located, or the assigned user simply no longer knows where the device is located.

SECTION: 1.0 GENERAL

SUBJECT: LOST OR STOLEN IT EQUIPMENT

D. Protected Information

Refers to information that is to be protected from improper disclosure or inappropriate use as defined by federal or state law, State Board of Education policy, or by LC State policy requirements. Compliance Standards including but are not limited to [Federal Educational Rights Privacy Act \(FERPA\)](#), [Gramm-Leach-Bliley Act \(GLBA\)](#), [Health Insurance Portability and Accountability Act \(HIPAA\)](#), Idaho Code section § [28-51-104](#)

E. Stolen device

Refers to a device that has been taken without permission or has been taken with permission but not returned in the agreed-upon timeline.

3. Policy

A. If the device is lost or stolen on college property:

The assigned device holder will, as soon as possible:

- i. Contact the LC State Department of Public Safety at 208.792.2226 and report the equipment as lost or stolen.
- ii. Contact their immediate supervisor in writing (email is the preferred method) and report the device as lost or stolen.
- iii. Complete the Missing Technology Asset/Device Report Form found on the LC State Information Technology page under Faculty and Staff Resources and email the completed form to the LC State College Help Desk at helpdesk@lcsc.edu.
- iv. If the device is known to be stolen or is reasonably suspected to have been stolen, file a police report with the appropriate legal authorities as directed by the LC State Department of Public Safety.
- v. Help Desk staff will contact the Cybersecurity Engineer and college Risk Manager via email.

B. IT Cybersecurity Engineer with the assistance of the Assistant Director of IT will:

- i. Contact the director of IT and LC State risk manager
- ii. Contact the device owner to determine the type of information stored on the device.
- iii. If confidential/restricted data were stored on the device, initiate the Information Security Incident Response Plan.
- iv. Follow the Tracking Stolen Computers procedures (an IT internal use document) and, if applicable, Computrace tracking procedures.
- v. Work with the LC State Department of Public Safety to ensure police reports are tracked and followed up on as required.

C. If Device is Lost or Stolen Off-Campus:

The device owner will, as soon as possible:

- i. Contact the LC State Department of Public Safety at 208.792.2226 and report the equipment as lost or stolen.
- ii. Contact local police authorities, provide details on the equipment, and request local police to contact LC State public safety regarding theft/loss.
- iii. Contact their immediate supervisor in writing (email is the preferred method) and report the device as lost or stolen.

SECTION: 1.0 GENERAL

SUBJECT: LOST OR STOLEN IT EQUIPMENT

- iv. Complete the Missing Technology Asset/Device Report Form found on the LC State Information Technology page under Faculty and Staff Resources and email the completed form to the LC State College Help Desk at helpdesk@lsc.edu.
 - v. Help Desk staff will contact the cybersecurity engineer and college risk manager via email.
- D. IT Cybersecurity Engineer with the assistance of the Assistant Director of IT will:
- i. Contact the Director of IT and the College Risk Manager
 - ii. Contact the device owner to determine the type of information stored on the device.
 - iii. If confidential/restricted data were stored on the device, initiate the Information Security Incident Response Plan.
 - iv. Follow the Tracking Stolen Computers procedures (an IT internal use document) and, if applicable, Computrace tracking procedures.
 - v. Work with the LC State Department of Public Safety to ensure police reports are tracked and followed up on as required.
- E. FOR ALL INSTANCES WHEN A DEVICE IS LOST OR STOLEN:
- If protected information was stored on the device and the Information Incident Response Plan is enacted, the director of IT will monitor the progress of the incident as managed through the Information Security Incident Response Plan and ensure that the college executive team is fully apprised of the incident and progress made as part of the resolution.

Authority:

[Idaho Code § 28-51-105](#) (Security Breaches)

[Federal Educational Rights Privacy Act \(FERPA\)](#)

[Gramm-Leach-Bliley Act \(GLBA\)](#)

[Health Insurance Portability and Accountability Act \(HIPAA\)](#)

[Idaho Code section § 28-51-104](#) (Identity Theft)