Information Security Incident Report Instructions

If you believe that an information security incident has taken place, please follow the following instructions to report the incident.

An information security incident is a violation or attempted violation of:
- District Information Security Policy (R-8870)
- International, Federal, State or Local Law/Regulations, or
- Unauthorized Data Access

Business Process Instructions:

1. Complete and submit the Information Security Incident Report form to your college/DO Information Security Officer.
   a. If the incident is related to a device still on the network, contact your college IT Department immediately. Do not make any other changes or updates to the machine.
   b. If the incident involves a lost or stolen computer/laptop, please also notify Campus Police.
2. Your college/DO Information Security Officer will contact you for more information if needed.

Form Instructions:

Fill out as much information about how you can be contacted and the nature of the incident. Attach additional pages to the form as necessary.

1. Incident Date/Time – Document the date and time the incident occurred or when you were notified/aware of the incident (if you do not know the exact date/time the incident occurred).

2. Type of Incident – Check all boxes that best describe the incident.

Type of Incident	Examples
Compromised Account	- Stolen password. - Password changed or reset without user knowledge. - Restricted data accessed and/or altered without user knowledge.
Compromised System	- Stolen password to account with access to IT systems (i.e. PeopleSoft, OGS, college servers, etc.). - Unauthorized access to IT systems. - Spyware/malware/key logging detected.
Lost or Stolen Computer/Laptop	Lost or stolen computer or laptop with protected information.

Type of Incident	Examples
Lost or Stolen Removable Storage	• Lost or stolen USB flash drive. • Lost or stolen CD/DVD with protected information (high risk or confidential data). • Lost or stolen external hard drive with protected information.
Unauthorized Access or Release of Protected Information ➢ Data that SHOULD NOT be made public and only accessed in a limited fashion. Information such as SSNs, DOB, student education records, benefits information, compensations, loans, health information, financial aid data, faculty and staff evaluations, etc.	• Lost/stolen documents with protected information. • Lost/stolen storage devices with protected information. • Unauthorized personnel reviewing protected information.

Copyright Infringement	• Unauthorized or prohibited use of works covered by copyright law.
	• Request for information due to illegal file sharing from:
	  ✓ Recording Industry Association of America (RIAA),
	  ✓ The Motion Picture Association of America (MPAA), or
	  ✓ The Digital Millennium Copyright Act (DMCA).

District Security Policy Violations	• Storing of high risks and confidential data on unsecure medium. • Sharing of passwords with other co-workers/supervisors. • Transmitting high risks and confidential data unencrypted.

3. **System Impacted** – Check all systems impacted by the incident.
4. **Description of Incident** – Include as much information as possible about the nature of the incident. This will help your ISO determines the level of risk of the information security incident.
5. **Names and Contact Information of Other Involved** – List the names and contact information of anyone else that may be involve in this incident or may be able to provide more information about the incident.

Submit the form to your college/District ISO. Current college/District ISOs are listed here:
http://www.losrios.edu/lrc/infosecurity.php