Procedural Directive

California State University
Northridge
Department of Police Services

To:	All Department of Police Services Personnel
Subject:	Information Security Lost or Stolen Device Reporting Procedures
Directive Number:	2008-04
Date:	December 18, 2019
Amends/Supersedes:	November 26, 2008 version; February 16, 2011 version; January 7, 2015 version.
Approved:	Gregory L. Murphy, Chief of Police

I. Objective:

This directive documents the reporting procedures required of patrol officers and investigators upon receipt of lost or stolen electronic device (e.g., computers, PDAs, memory sticks, cell phones, etc.) which contain or may contain confidential/sensitive university-related information. (Note: California State University, Northridge identifies protected data within the following web address: http://www.csun.edu/it/security/protecteddata.html.) This procedural directive works in conjunction with Department Policies #07-C.I.-005: Criminal Investigation, #05-C.I.-001: Case Screening & Case File Management Systems, #07-O.A.-007: Field Reporting and Management, and #07-O.A.-006: Records Administration.

II. Procedures:

A. Preliminary Investigation

Upon receipt of a lost or stolen electronic device report/investigation, officers are to ask the following questions which will assist CSUN Information Security determine the steps required to respond to a lost or stolen electronic mobile device report and the potential compromise of university protected data.

1. What was the primary purpose or function of the stolen device?

2. Did the lost or stolen device contain University student confidential/sensitive information (e.g., names, SSN, birth dates, PIN numbers, usernames, passwords, home address, etc.)?
3. Did the lost or stolen device contain University staff or faculty confidential/sensitive information (e.g., SSN, birth dates, PIN numbers, usernames, passwords, grades, home address, etc.)?
4. Did the lost or stolen device contain Payment Card Industry information? (e.g., credit card information, back account information, PIN numbers, etc.)

"Yes," "No," or "Unsure" shall be used to answer #2, #3, and #4 of the above questions. If the answer is "yes" or "unsure" to any of the questions, officers are to provide detailed information regarding the potential loss of confidential/sensitive information within a police report and ensure that the following notification requirements are made. A "no" response also requires a police report, however only those involving state owned/controlled property (both physical and intellectual property) need to be forwarded by the records unit to the university CIO, ISO, Internal Auditor, and Asset Manager.

B. Notification Procedures

Dispatch: Upon receipt of a report involving a lost or stolen electronic device, dispatch shall inquire whether or not the equipment is state property and if so, what campus department the item(s) belong to. A police officer shall be assigned to conduct a preliminary investigation of the reported lost or stolen item.

Police Officer (Preliminary Investigator): The preliminary investigator shall follow the directives set forth within this procedural directive as well as the department's preliminary investigation policy. He/she shall also notify the shift supervisor of the incident and advise him/her whether or not sensitive information was contained within the lost or stolen electronic device.

Shift Supervisor and Management Response: The police shift supervisor shall immediately notify their respective Patrol Operations Commander of any loss or potential loss of university sensitive/protected data (as defined by the CSU at the website above). Should the loss report be made after 2200 hours and the lost information not be deemed "critical (e.g., passwords detrimental to the university's IT systems)," notification of the respective Patrol Operations Commander (if not on duty) and Chief of Police may be made between 0500 to 0600 hours the following day. The Patrol Operations Commander will notify the Chief of Police and either she/he or her/his designee will contact the university Chief Information Officer (CIO) and Information Security Officer (ISO) of the situation. The Patrol Operations Commander or his/her designee will contact the university Internal Auditor, Asset Manager, and Special Services Captain.

Detectives (Follow-Up Investigator): The University Police Investigations Unit shall initiate follow-up investigation procedures for **ALL** state owned/controlled lost or stolen electronic mobile devices and private entity devices where a potential loss of university protected data exists. All case screening and case file management criteria used to justify classification of the case, as well as any follow-up investigation work completed, shall be documented within a supplemental report. This report shall document the formal case review, response, and investigatory measures taken by department investigators.

Records Supervisor: Once all applicable report(s) are approved by the shift supervisor, the records supervisor will finalize the processing of said reports within RIMS. Copies of those preliminary and follow-up investigation reports involving state owned/controlled property (i.e. both physical and intellectual property such as a state owned computer or state controlled electronic data that may be contained within a personal computer) will be sent to the university CIO, ISO, Internal Auditor, and Asset Manager only after receiving approval from the Chief of Police or her/his designee.