DCRI Standard Operating Procedure:

NIH Clinical Center Standard Operating Procedures for Lost or Stolen CC IT Device(s)

Procedure\Process Number: CC-DCRI-S2015-01

Version 1.0

August 10, 2015

NIH Clinical Center

National Institutes of Health

Document Control

Abstract:	
Process Number:	CC-DCRI-S2015-01
Author / Process Manager:	Jothi Dugar
Process Owner:	DCRI
Approved By:	Jon W. McKeeby, DCRI Department Head
Effective:	8/10/15
Version Number:	1.0
Next Scheduled Review:	One year from the last approved date.

The latest approved version of this document resides on the DCRI website

Change History

Version	Date of Issue	Author(s)	Description of Change(s)
0.20		CC Policy Committee	Initial draft for general review
0.40		Jothi Dugar, Jon W. McKeeby, Jim Pitts	Draft for general review
0.60		Jothi Dugar, Jon W. McKeeby, Jim Pitts	Draft for general review
1.00	8/10/15	Jothi Dugar, Jon W. McKeeby, Jim Pitts	First release
1.10	8/10/15	Jothi Dugar, Jon W. McKeeby, Jim Pitts	Second release, addresses comments on first release
1.20			

Table of Contents

[Page intentionally left blank]

1 Purpose

To provide procedures to report lost or stolen government furnished IT device(s) and/or storage media, whether or not the device(s) contains sensitive or Personally Identifiable Information (PII).

2 Scope

This document addresses the procedures to be used and roles and responsibilities if/when a Clinical Center IT device has been lost and/or stolen in accordance with the NIH Procedures for Lost or Stolen Devices.

3 Applicability

The procedures described in this document apply to all CC users with government owned IT device(s) to include but limited to: smart phones, tablets, and/or other portable media.

5 Roles and Responsibilities

The roles and responsibilities of the participants are outlined in the following table.

ROLES	RESPONSIBILITIES
CC Information Security Office (CC ISO)	Responsible for completing Incident Reports in the NIH IRT Portal, verifying that Department Property Custodial Officer has been contacted, and CC Mobile Device Management Team has been notified to perform security wipe
CC Mobile Device Management Team	Responsible for conducting secure wipe for mobile devices managed by the CC
CC Administrative Officer	Responsible for assessing department/office budgets when replacement devices are needed and ensuring that internal property lists are kept up to date
CC Property Management/Property Custodial Officer (PCO)	Responsible for ensuring that service/data plans are shut off and issuing new device to user as needed

ROLES	RESPONSIBILITIES
NIH CIT	Responsible for creating service tickets and IRT Portal incidents and routing to CC ISO for CC managed devices; also responsible for conducting secure wipe of devices managed by NIH CIT and reporting incident to all respective Privacy offices if PII was compromised
User	Responsible for communicating and coordinating new nurses training classes, requests for CRIS SCM account creation, and modification and inactivation for Nursing and Patient Care Services (NPCS) department staff.
CRIS Core Security Administrator (DCRI Security Lead)	Responsible for reporting the incident as outlined in this SOP to the respective authorities

6 Background Information

The Office of Management and Budget (OMB) presidential memo (OMB-06-016) requires that federal agencies report incidents of stolen PII to the US-Computer Emergency Readiness Team (CERT). This procedure describes how IT devices and media at NIH are to be handled.

Examples of Portable Equipment include:

- IT Devices (e.g., Laptop, Smartphone, Tablet, Camera)
- Media (e.g., Hard Drive, USB/Thumb Drive, Secure Digital Media Card, CD-ROM, etc.)

Examples of PII (Personally Identifiable Information) contained in IT Systems include:

- Background investigation paperwork (i.e., name, job history, clearances held)
- Clinical research data (i.e., race, national origin, gender, age, disease diagnosis)
- Confidential financial disclosure forms (i.e., name, stocks, bonds, assets, liabilities)
- Grant application (i.e., name, Principal Investigator number, and proprietary data)
- Patient medical record (i.e., MRN, SSN, gender, ethnicity, diagnosis/treatment/medications)
- Police report (i.e., license plate number, criminal allegations, insurance claim info)
- Travel order/voucher (i.e., travel itinerary, personal relocation expenses).

7 Procedure

1. If a user determines that a CC IT device(s) is stolen, the user must report the event to the NIH police, OR to the local police if off campus, **within one hour** of discovering that the device has been stolen. If the user determines that a CC IT device(s) has been lost, user shall proceed to step 2 below,as police report is not required for lost devices.

2. The user must also:

   a) Notify their supervisor, Administrative Officer and the NIH IT Service Desk of the lost or theft of the device(s) by calling either at 301-496-4357 or 1-866-319-4357 or email IRT@nih.gov.

   b) Complete HHS Form 342 Report of Survey. (See Appendix A for sample; form is available from the CC DCRI Inventory & Property Management Team.)

   c) Send copy of police report ***(for stolen devices; lost devices do not need police report)*** and a completed HHS Form 342 to the Department Property Custodial Officer (PCO) and to the CC Information System Security Officer (ISSO)

3. The NIH IT Service desk immediately informs the IRT by phone at 301-881-9726 or email at IRT@nih.gov.

   a) If the IT device is managed by NIH, the NIH IT Service Desk will immediately issue a kill-command and perform a security wipe the next time the device is on line.

   b) Creates the initial IRT Portal incident ticket and routes the ticket to the CC ISSO.

   c) If PII was compromised, IRT will report the incident to Secure One HHS within one hour of discovery and notifies the HHS Cybersecruity Program by phone and/or email who will then notify HHS PIRT as appropriate.

4. The CC ISSO will create a ticket to the CC Mobile Device Management team to wipe the device if managed by the CC.

5. The CC Mobile Device Management Team will issue a Wipe command for any mobile device managed through the CC mobile device management program within 24 hours of notification.

6. The CC ISSO and/or Privacy Coordinator completes the incident report in the IRT Portal, updates it as more information becomes available, and uploads all relevant documents (i.e., police report ***(for stolen devices only)***, HHS Form 342, Breach Response Plan, and Notification Letter to the affected individuals).

a) If PII was compromised, the NIH Senior Official for Privacy (SOP) and the CC Privacy Coordinator are notified by NIH by creation of the IRT Portal ticket which triggers NIH Breach Response activities.

b) None of the documents uploaded to the IRT Portal should contain any of the PII lost as a result of the incident. If for instance, the police report contains the victim's name, gender, home address, the **PII must be redacted before the document is updated to the IRT Portal.**

c) The CC ISSO will ensure that the CC DCRI Inventory & Property Management Team has been notified if loss/theft/damage of the government property is involved.

d) The CC Inventory & Property Management will ensure any service/data plans for the lost/stolen device are shut off and will issue the user a new device as needed.

7. The Administrative Officer assesses the department/office budget to ensure funds are available for replacement devices. Also assures that internal department/office property lists are updated.

8 Breakdown of Responsibilities for Lost/Stolen CC IT Devices

User Responsibilities	CC ISSO Responsibilities	NIH Responsibilities	CC Property Management/PCO Responsibilities	CC Administrative Officer	CC Mobile Device Management Team
User discovers GFE computing device/media is lost/stolen	CC ISSO routes the Service Now ticket from NIH to CC Mobile Device Management Team to wipe the device if managed by the CC	NIH creates Service Now ticket and routes it to CC Security Team	Dept. PCO ensures any service/data plans for device are shut off	Assesses budget to ensure funding available for replacement devices	Issues a Wipe command for mobile devices managed by the CC within 24 hrs. of notification
User reports theft to law enforcement (NIH Police if on campus or local police jurisdiction if off campus) within 1 hour and obtains police report (only for devices that were stolen; lost devices do not require police report)	CC ISSO and/or CC Privacy Officer completes Incident Report in the NIH IRT Portal, updating as more information becomes available, and uploads all documents (e.g. Police Report, HHS Form 342, Breach Response Plan and Notification Letter to Affected Individuals) if PII leaked	NIH creates an IRT Portal Incident and routes to CC ISSO Team	Dept. PCO will issue user a new device as needed	Updates internal dept./office property lists	
User reports incident to Supervisor and Administrative Officer	CC ISSO verifies that Dept. PCO has been notified of the loss/theft of GFE	If device managed by NIH, NIH issues kill command and performs security wipe of device	Dept. PCO sends the HHS Form 342 and police report to CC Property Staff/ Section to have device removed from Dept. inventory		
User/Supervisor reports loss/theft within 1 hour to NIH IT Service Desk (301-496-4357 or 866-319-4357) or via email (IRT@nih.gov)		If PII compromised, NIH reports incident to SecureOne HHS, notifies Cybersecurity Program and HHS PIRT. NIH SOP and CC Privacy Officer notified via creation of IRT Portal Incident			
User obtains (via policy or CC Property Staff/Section) and completes HHS Form 342					
User sends copy of HHS Form 342 and police report to Dept. PCO and CC ISSO Team					

Appendix A - References

1. OMB-06-016, Memorandum for the Heads of Departments and Agencies, Executive Office of the President, 6-23-06.

2. CC Administrative Policy Manual, I-001, Management of Mobile Cellular Devices.

3. CC Administrative Policy Manual, I-002, CC Skype Policy.

4. NIH Policy Manual Chapter 2813 NIH Information Security Awareness and Training Policy.

Appendix B – HHS Form 342

DEPARTMENT OF HEALTH AND HUMAN SERVICES

FORM HHS-342
(8/01)

REPORT OF SURVEY

(See Instructions § 103-27.57
HHS Logistics Management Manual)

REPORT NUMBER

DATE OF REPORT

PAGES IN REPORT

Subpart 103-27.57-Board of Survey Procedures
103-27.5700
This subpart describes the Board of Survey Process that will be used by components of the Department to investigate losses, damage and destruction of government property, to establish liability for the loss or damage and to provide relief from accountability.

1.

TO:

2. INDICATE ACCOUNTABLE AREA INVOLVED

3. THE ITEMS LISTED BELOW WERE:

☐ LOST ☐ SHORT ON INVENTORY
☐ DAMAGED ☐ DESTROYED ☐ OTHER

IDENTIFICATION OR ITEM NUMBER	DESCRIPTION OR NOMENCLATURE	UNIT	UNIT COST	QUANTITY	TOTAL COST
					GRAND TOTAL

4. EXPLANATION (See Instructions)

Initiator _____ (Signature) _____ (Title) _____ (Date)

5. ADDITIONAL INFORMATION (See Instructions)

Prop. Mgmt. or Accountable Officer _____ (Name) _____ (Title) _____ (Date)

Created by: PSC Media Arts (301) 443-2454 EF

Appendix C – Definitions

1. ***Personally Identifiable Information (PII):*** any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

2. ***Service Now ticket:*** service tickets that are created and managed via the NIH Service Now IT Service Management System.

3. ***IRT Portal Incident:*** tickets that are created and managed via the NIH IRT Portal for any security and privacy incidents.

4. ***Wipe or "Kill" Command:*** a series of commands used to clean or sanitize data or to completely over write all of the data on a hard drive.