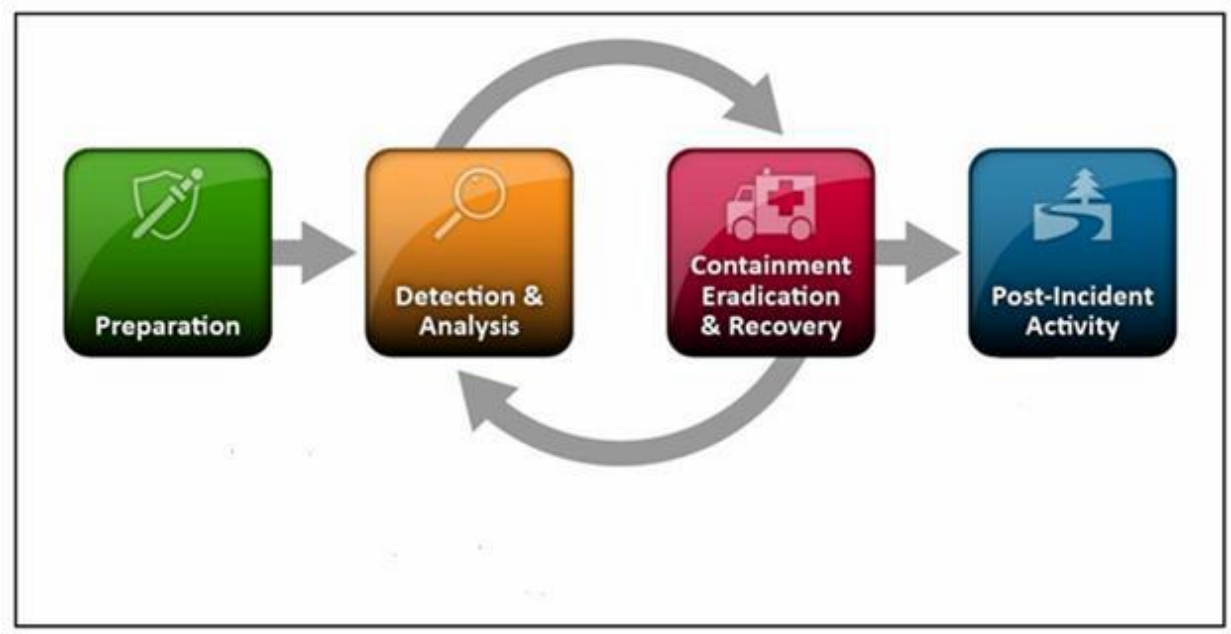
Information Technology Security and Privacy Incident Response and Reporting Procedures

Florida State University
Information Security and Privacy Office (ISPO)
2014

Florida State University

Information Technology Security Incident Response and Reporting Procedures (July 2014)



From NIST Computer Security Incident Handling Guide, Special Publication 800-61

1.0 Overview of IT Security Incident Response and Reporting

Information Technology (IT) Security Incident Response and Reporting is tied to the principal University goal for information security: preserving the confidentiality, integrity and availability of enterprise information assets. An effective IT Security Incident Response program provides a means of dealing with unexpected circumstances in such a way as to minimize impact to the University. It also provides management with sufficient information on which to base an appropriate course of action.

A systematic IT Security Incident Response program utilizing a formal methodology offers several benefits to the University such as:

- Providing a structured, logical approach to use in situations that are usually chaotic.
- Increasing the efficiency of dealing with an incident, which reduces the impact to the University from both financial and human resources (HR) perspectives.
- Providing evidence of due diligence and forethought that may become significant should legal and liability issues arise following an incident. This is particularly true when dealing with disclosure regulations and compliance with laws.

The University has established policies requiring action by campus IT administrators to report and respond to IT security incidents. Selected text from OP-H-9 Information Technology Security Policy, OP-D-2-G Payment Card Policy, and OP-H-9 Primary Identifier Policy defines the following courses of action with the discovery of an IT security incident:

- The unit IT/Information Security Managers (ISMs) must immediately notify the FSU IT Security Incident Officer of IT security incidents within their units, especially those that may be threatening to other IT resources (e.g., hacking of a mail or web server).

- In the event of a payment card data security breach, the department head should be notified immediately of any suspected or real security incidents involving computing assets, particularly any critical system. If it is unclear as to whether a situation should be considered a security incident, the department should coordinate with their departmental IT Security Manager to evaluate the situation. Subsequent to that evaluation the departmental IT Security Manager should escalate and notify the university Information Security Manager of the incident.

- Unit IT/ISMs should notify the FSU Police Department (FSUPD) about IT security incidents involving threats to human beings, property, child pornography, or incidents involving a breach of Criminal Justice Information Services (CJIS) information.

- External law enforcement entities (FBI, FDLE, other federal, state, local law enforcement entities) must be referred to the FSUPD who will serve as Liaison during all IT security investigations (e.g., use of computing resources to commit credit card fraud).

- The FSU Office of General Counsel, Director of Information Security and Privacy, and FSUPD must be notified when a subpoena is issued pursuant to any investigation related to information technology.

- Inadvertent release or compromise of sensitive data, including the loss or compromise of portable computing devices or removable media containing sensitive data, or the discovery of unauthorized access to sensitive data on a computer or data storage device, must be reported immediately to the respective VP, Dean, Department Head, Director, and campus police. Upon discovery of the unauthorized computer access, campus units must report the incident to abuse@fsu.edu as soon as possible after discovery. If the campus unit does not have existing internal capability to conduct computer analysis and related forensics, members of the FSU IT Security Incident Response Team (FSU ITSIRT) will begin (in direct collaboration and coordination with the campus unit Department head and IT lead) an investigation as to the cause of the incident, and recommend to the appropriate Vice President, Dean, Department Head, or Director the appropriate corrective action to be immediately taken to terminate unauthorized access and prevent a recurrence of the loss of data integrity.

2.0 Departmental Responsibilities for Reporting and Responding to an IT Security Incident

2.1 Reporting of IT Security Incidents

There are many different kinds of IT Security Incidents and different departments will

become involved in the remediation of the incidents. It is the responsibility of the department to report an incident to the appropriate department. Anything considered criminal activity should be reported to the FSUPD. Employee misconduct, both criminal and otherwise should also be reported to Human Resources. Incidents of a technical nature usually deriving from an external source should be reported to the FSU Director of Information Security and Privacy.

All University data, regardless of the format or medium of the record (paper, electronic data/voice/video/image, microfilm, etc.), should be classified into one of three sensitivity levels categories:

Level 1 - Protected

Level 2 - Private

Level 3- Public

The data classification level of information involved in an incident is an important component in the process of timely risk mitigation in the response process.

2.1.1 Types of IT Security Incidents Reported to FSUPD

1. Electronic transmission/storage of child pornography
2. Electronic transmission of threats to the physical safety of human beings or physical assets
3. Harassment and other criminal offenses involving individual user accounts
4. Loss or theft of computing device
5. Use of FSU computing resources in the commission of a fraudulent activity against the University, individual, or outside entity. Suspected fraud activities may also be reported to the University's Ethics Point hotline at (855-231-7511) or the FSU Ethics Point website.
6. Incidents involving a breach of Criminal Justice Information Services (CJIS) information

2.1.2 Types of IT Security Incidents Reported to Human Resources (Employees/Faculty) or Office of Student Rights and Responsibilities (Students)

Misuse of FSU IT resources is thoroughly described in OP-H-6 and some common examples are listed below.

1. Commercial use of IT resources that is not pre-approved
2. Advertisements for personal gain on fsu.edu websites

3. Use of IT resources that interferes with the performance of employee's job

4. Use of IT resources that result in an incremental cost to the University

2.1.3 Types of IT Security Incidents Reported to Meet Criminal Justice Information Systems (CJIS) Incident Response Requirements

1. Campus units maintaining an agreement with Florida Department of Law Enforcement (FDLE) to access, process, or store Criminal Justice Information (CJI) protected information shall promptly report any breach of security or privacy of this information to the appropriate authorities as directed in CJIS Security Policy 5.2 (Section 5.3 Policy Area 3: Incident Response).

2. A user of a CJIS system who knows or suspects that a security incident has occurred is responsible for informing the user's supervisor immediately.

3. Supervisors are required to notify their Dean/Director/Department Head, Director of Information Security and Privacy, the Inspector General, the Terminal Agency Coordinator (TAC), and the Local Agency Security Officer (LASO) in the Florida State University Police Department of any suspected security incident involving CJI and/or a CJIS system.

4. In addition to making notifications as directed in this incident response procedures guide; the LASO and/or TAC is responsible for ensuring the FDLE Information Security Officer (ISO) is immediately notified.

5. The LASO is responsible for collecting and logging information concerning the incident.

2.1.4 Types of Major IT Security Incidents Reported to the FSU Director of Information Security and Privacy

1. Personally Identifiable Information (PII) - The University is required by various State (Florida Statute 501.171), Federal regulations (FERPA, HIPAA, GLB) and contractual obligations (PCI DSS) to investigate any incident that may involve the breach of personally identifiable information. The University may also be required to notify an individual if the privacy of a combination of unencrypted contractual obligation has been breached. The dean, director, or department head of the area involved in the IT security incident may be responsible for coordinating any legally or contractually mandatory breach notices in cooperation with the University General Counsel.

2. Root or system-level attacks on mission critical Information System(s) desktop, laptop, smartphone, tablet, server, storage device or on any part of the supporting network infrastructure, e.g., switches, wireless access points, routers.

Unauthorized root access on a computing or storage device may allow the user read, write, and update capabilities over data, applications, and the security settings of the device. Unauthorized root access on a network communications device may allow the intruder the ability to intercept unencrypted communications, reroute network traffic to unintended devices, change device security settings, or conduct denial of service attacks.

3. Root or system-level attacks on any FSU owned computing device, e.g. server, workstation, tablet, or smartphone which the authorized user may use to conduct University business with data classified as "Protected" or "Private" information or to authenticate into critical University systems and may store data on the device.

4. Compromise of restricted protected service accounts or software installations, in particular those used for IT applications containing data classified as "Protected" or "Private", or those used for system administration.

5. Denial of service attacks that impair the availability of FSU computing resources.

6. Malicious code attacks including malware infections on devices that may allow an unauthorized user the ability to bypass system security controls on systems accessing, transmitting, or storing data classified as "Protected". In addition, vulnerabilities in applications code that may be used to bypass security controls to change application security settings, access supporting database(s) storing "Protected" data, or reroute users to an unauthorized site.

7. Open mail relay used to forward spam or other unauthorized communications associated with a University e-mail account.

8. Compromise of user logon account credentials that might be or have been used to circumvent logical security controls of University applications including, but not limited to; Oracle/SQL Server, Blackboard, OMNI, Campus Solutions, NWRDC mainframe applications, and E-mail accounts.

9. Denial of service on individual user accounts

10. Other-An attack that does not fit into any of the above categories but constitutes a risk to the confidentiality, integrity, or the availability of University systems or data.

2.1.4 Types of Minor Security Incidents

1. Virus infections on severs and end-points that do not contain data classified as "Protected" or "Private" or are not used to process "Protected" or "Private" data in a public location such as a kiosk.

2.2 Departmental Response to IT Security Incidents

2.2.1 Isolation and Protection of Compromised Device(s)

When there is suspicion of a breach in the security or privacy of a University owned computing device, the following steps should be taken. Failure to follow industry-standard computer investigation procedures can invalidate the collection of potential evidence.

- Discontinue use of that device immediately
- Do not power off the device as this could delete useful information for an investigation.
- Disconnect the network cable at the network jack in the wall or switch
- Isolate the computer to prevent any further use.
- Preserve logs on any devices in system or network to aid in forensic analysis
- Depending on the type of suspected compromise, contact the FSUPD, HR, or the FSU IT Security Incident Officer to assist in the investigation.

2.2.2 Identification of Personally Identifiable Data

Analyzing what data and applications might have been potentially exposed is an important component of the incident response process. System administrators and functional application/data owners of the devices should have an accurate inventory of the data on the compromised, lost or stolen device(s). If this information is not available, ISPO has software that can discover and classify the type of data on certain breached devices to develop an appropriate response plan. This service requires the delivery of the media to ISPO for processing, so it is only useful for removable media. Lost or stolen device backups may be scanned when the physical device is no longer available.

2.2.3 Calculation of Campus Unit Fiscal Cost to Remediate Incident

It is the responsibility of the University to quantify the total cost involved in the incident response process for legal purposes. All entities/personnel involved in the response process should maintain adequate records to fulfill this task including:

1) Create an inventory of all responder hours spent working the incident both on the technical and administrative levels;
    a. Providing detailed information on the specific work assignment for the responders;
2) Reporting any hours spent by faculty or staff in the remediation process including lost productivity of users;

3) Engaging affected FSU users to determine hours spent resolving issues related to the incident such as password resets, filing police reports, or loss of productivity should their FSU computing device require reimaging or a forensic examination.
4) Recording any 3rd party costs if outside entities are contracted to assist in forensic or technical assistance during remediation.

APPENDIX A contains an example of a master worksheet. Each campus unit will maintain a subsidiary worksheet similar to the master worksheet for submission to ISPO at the conclusion of the remediation effort.

3.0 Responsibilities of the FSU IT Security Incident Response Team (FSU ITSIRT)

Creating an interdisciplinary IT Security incident response team that is drawn from all parts of the enterprise and is educated and prepared to respond to events is a key component of a comprehensive IT Security incident response program. The FSU ITSIRT is directly responsible for providing information and assistance to members of the University community when responding to incidents.

Each incident could require various FSU constituents and personnel to be available for investigation and remediation. The Director of Information Security and Privacy in coordination with the CIO will select from the organizational units deemed technically proficient to provide their expertise to the particular incident. The following University organizational units may be convened depending on the incident reported.

Function/Incident Type	Campus Unit
Direction and oversight for IT issues	CIO
Campus PCI Compliance	Controller's Office
Computer Forensic expertise	ITS Information Security and Privacy Office
Physical forensic expertise	FSU Police Department
Enterprise network security expertise	ITS Network Communication Technologies
Physical security/public safety	FSU Police Department
Overall direction campus emergency response plan	Emergency Management Coordinator
Restricted Research Data (ITAR) (EAR)	Export Control Officer
HIPPA data incident	Local HIPAA Privacy Officer
Windows and Virtual Machine supported data environment	ITS Infrastructure and Operations
Unix/Linux supported data environment	ITS Infrastructure and Operations
OMNI/Campus Solutions	Enterprise Resource Planning
Data storage	ITS Infrastructure and Operations
Employee data incident	Human Resources
Student (FERPA) data incident	Division of Student Affairs/Admissions and Records
Financial aid, registration, or admission data incident	Controller's Office/Admissions and Records
Expertise within departmental IT environment	Department System Administrators
Public communications and responses to press inquires	University Communications
Regulation and policy expertise	Inspector General/General Counsel/ITS Information Security and Disaster Recovery

The FSU ITSIRT will only engage in Human Resource cases upon the request of the Office of Human Resources or the FSUPD and under the direction of the University's IT Security Incident Officer. Select use violations are stipulated in University OP-H-6 Information Technology Use Policy.

The FSU ITSIRT is authorized to address all types of computer security incidents that might occur at FSU. Response will be prioritized based on the following relevant factors.

- ✓ Functional impact – negative impact on University functions
- ✓ Informational impact – confidentiality, integrity, and/or availability of data
- ✓ Recoverability – time and resources that must be allocated to recover from the incident

The FSUPD will act as a liaison for any incident/event requiring contact with outside law enforcement agencies to ensure the proper agencies are contacted to prevent jurisdictional issues

4.0 IT Security Incident debriefing

4.1 Lessons Learned

One of the most important parts of incident response is also the most often omitted: learning and improving. Each incident response team should evolve to reflect new threats, improved technology, and lessons learned. Holding a "lessons learned" meeting with all involved parties after a major incident, and optionally periodically after lesser incidents as resources permit, can be extremely helpful in improving security measures and the incident handling process itself. Multiple incidents can be covered in a single lessons learned meeting. This meeting provides a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked. The meeting should be held within several days of the end of the incident.

Questions to be answered in the meeting include:

- ➢ Exactly what happened, and at what times?
- ➢ How well did staff and management perform in dealing with the incident?
- ➢ Were the documented procedures followed?
- ➢ Were they adequate?
- ➢ What information was needed sooner?
- ➢ Were any steps or actions taken that might have inhibited the recovery?
- ➢ What would the staff and management do differently the next time a similar incident occurs?
- ➢ How could information sharing with other organizations have been improved?
- ➢ What corrective actions can prevent similar incidents in the future?
- ➢ What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

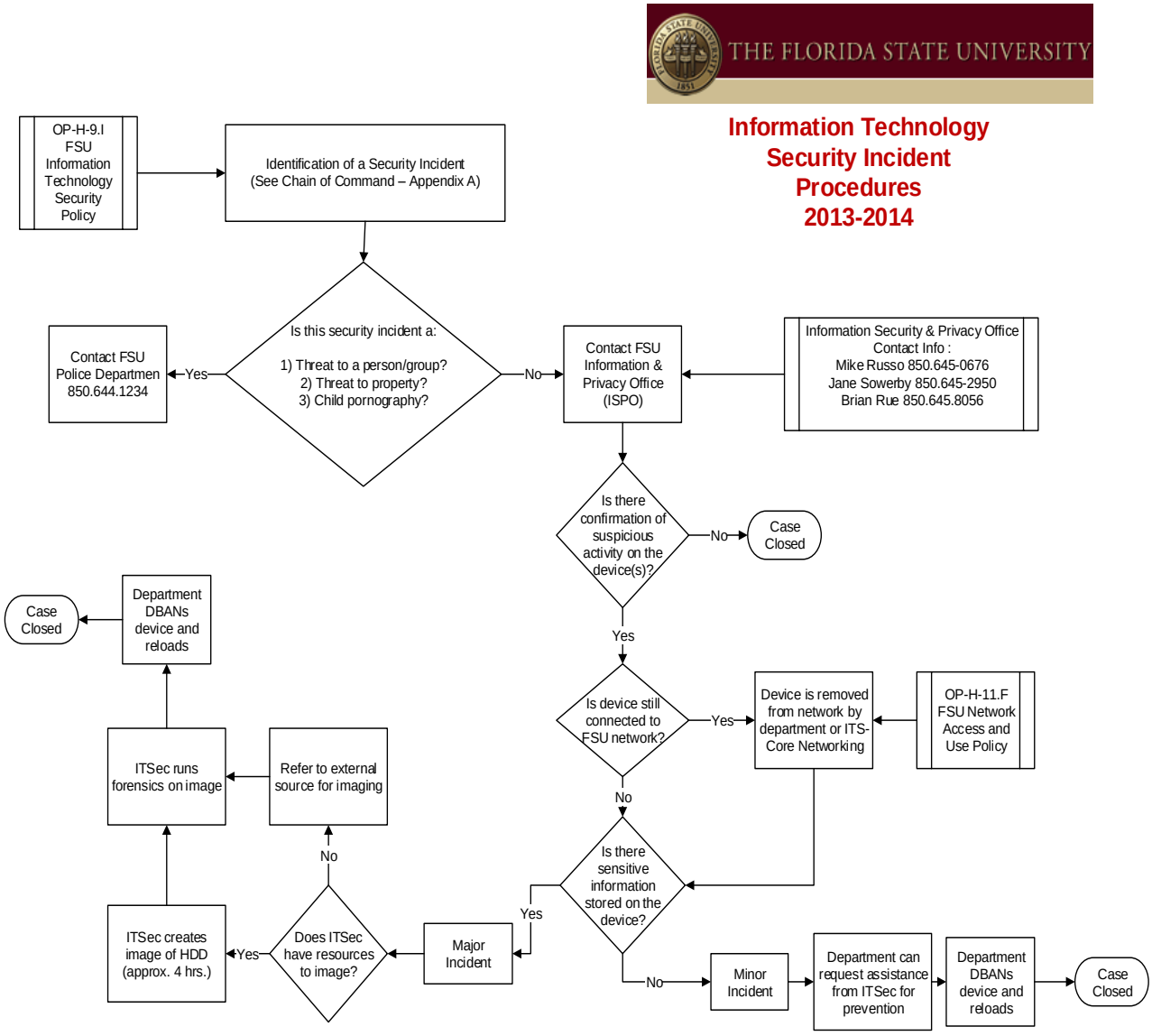
4.2 IT Security Incident Report Creation and Distribution

The members of the FSU ITSIRT who are involved in the remediation of an incident classified

as a major event will create a report. The report will be available to the campus unit administrator, dean, director, or department head at the discretion of the Director of Information Security and Privacy or University Chief Information Officer.

4.3 Media Contact

University Communications will be responsible for disseminating information on University IT security incidents with the media. Please refer any information requests concerning an IT security incident to this group as a single point of contact. Ensure your staff understands this procedure.



APPENDIX A

Example of the master incident response cost spreadsheet:

FSU CSIRT - Resolution of Final Costs

Responders Costs				
Job Title	**Number of Responders**	**Hours**	**Cost/Hour**	**Total**
Example: Technology Specialist	2	100	25	$5,000.00
Example: Campus Unit Director	1	20	68	$1,360.00
Example: Network Engineer	3	60	56	$10,080.00
				$0.00
Subtotal	6	180	149	$16,440.00
Benefits @28%				$4,603.20
Subtotal (Salary and Benefits)				$21,043.20
Indirect Costs (building/heat/cooling) 52% of Salary/Benefits				$10,942.46
Total Labor Cost				**$31,985.66**

Faculty/Staff Users Cost				
User Type	**Number of Users**	**Hours Lost**	**Cost/Hour**	**Total**
Example: Professor	5	30	$75.00	$11,250.00
Example: Graduate Student	2	11	$25.00	$550.00
				$0.00
Subtotal	7	41	$100.00	$11,800.00
Benefits @28%				$3,304.00
Total User Cost				**$15,104.00**

Total Incident Cost	
User Type	**Total**
Responders Cost	$31,985.66
Faculty/Staff Users Cost	$15,104.00
Total Incident Cost	**$47,089.66**