FSU | INFORMATION TECHNOLOGY SERVICES

Cyber and Information Security Incident Response and Reporting Procedures
Working Copy

Table of Contents

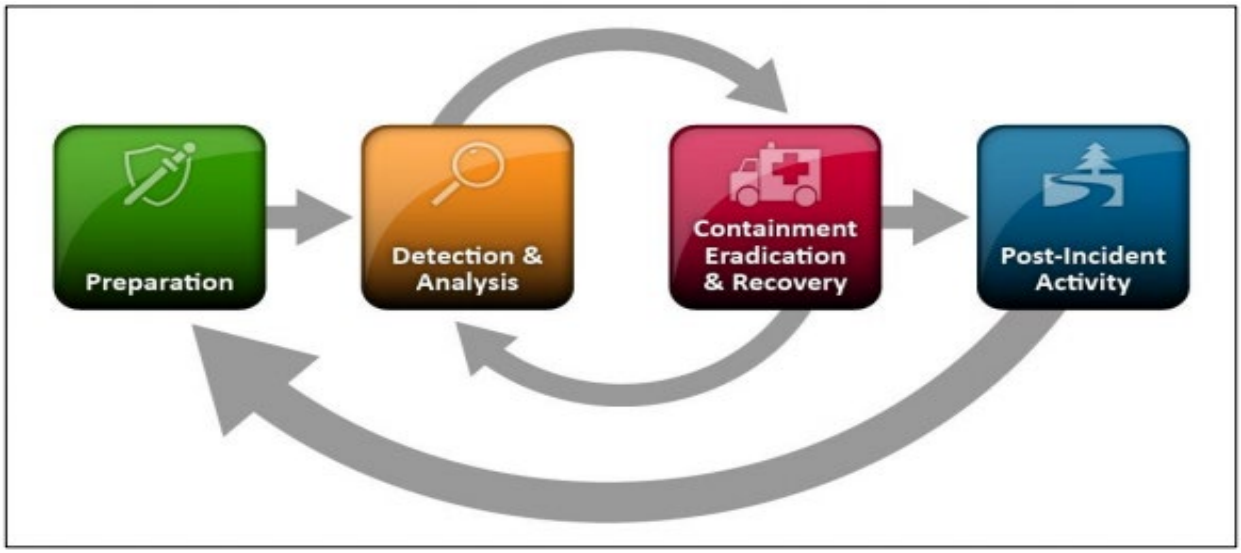
1.0 Overview of IT Security Incident Response and Reporting 5
1.1 Cybersecurity Risks 5
1.2 Cybersecurity Best Practices 6
2.0 Cyber and Information Security and Privacy Process Description 8
2.1 Incident Identification 8
2.1.1 Overview 8
2.1.2 Incident Types 8
2.1.3 Incident Symptoms 8
2.2 Incident Assessment 9
2.2.1 Overview 9
2.2.2 Considerations 9
2.2.3 Documentation 9
2.3 Incident Reporting and Communications 9
2.3.1 Reporting Cybersecurity Incidents and Communication Guidelines 9
2.3.2 Information Security and Privacy Office Intelligence Services 10
2.3.3 Incident Communication Guidelines 11
2.4 Incident Response 12
2.4.1 Briefing of Administration 12
2.4.2 Initial Response 12
2.4.3 Remediation and Recovery 13
2.5 Incident Report 13
2.5.1 Overview 13
2.5.2 Incident Report Contents 13
2.5.3 Timeframe 14
2.6 Incident After Action Review 14
2.6.1 Post-Incident / After Action Review Meeting 14
2.6.2 Process Improvement Plan 14
3.0 Reporting and Responding to Cyber or Information Security Incidents 15
3.1 Reporting of Cyber and Information Security Incidents 15
3.1.1 Types of IT Security Incidents Reported to FSUPD 16
3.1.2 Types of IT Security Incidents Reported to Human Resources 17
(Employees/Faculty) or Office of Student Rights and Responsibilities (Students) 17
3.1.3 Types of IT Security Incidents Reported to CJIS (Criminal Justice Information Systems) Incident Response Requirements 17
3.1.4 Types of Major Cyber or Information Security Incidents Reported to ISPO 17

3.1.5 Types of Minor Security Incidents 18
3.2 Departmental Response to IT Security Incidents 19
3.2.1 Isolation and Protection of Compromised Device(s) 19
3.2.2 Identification of Personally Identifiable Data 19
3.2.3 Calculation of Campus Unit Fiscal Cost to Remediate Incident 19
4.0 Responsibilities of FSU CSIRT (FSU Cyber and Information Security Incident Response Team) 20
4.1 Cyber and Information Security Incident debriefing 21
4.1.1 After Action Analysis and Lessons Learned 21
4.1.2 Cyber and Information Security Major Incident Report Creation and Distribution 22
Appendix A – Security Incident Runbooks 23
Security Incident Category: MALWARE / MALICIOUS CODE / SPYWARE 24
Coordinating Units 24
Preparedness 24
Response 25
Security Incident Category: PHISHING/SOCIAL MEDIA 26
Coordinating Units 26
Preparedness 26
Response 26
Security Incident Category: COMPROMISED CREDENTIALS 27
Coordinating Units 27
Preparedness 27
Response 27
Security Incident Category: DEFACEMENT / WEBSITE SECURITY 29
Coordinating Units 29
Preparedness 29
Response 29
Security Incident Category: DATA BREACH 31
Coordinating Units 31
Preparedness 31
Response 31
Security Incident Category: DENIAL OF SERVICE / DISTRIBUTED DENIAL OF SERVICE 33
Coordinating Units 33
Preparedness 33
Response 33
Security Incident Category: FERPA INCIDENTS 35
Handling of FERPA Incidents 35

Appendix B – Incident Communication Templates 37
Parent or Guardian Template 37
Faculty/Staff Template 38
External Communication Template 39
External Source of Unauthorized Disclosure Form 40
Appendix C – Standards: Information Technology Services 41
Appendix D – Technology: Policies and Procedures 42

1.0 Overview of IT Security Incident Response and Reporting

IT Security Incident and Response and Reporting Cycle



Incident Response Recommendations and Considerations for Cybersecurity Risk Management: NIST SP 800-61r3

1.1 Cybersecurity Risks

The Information Security and Privacy Office (ISPO) has categorized the top cybersecurity risks that University Information Technology Professionals, Information Security Managers, and Unit Privacy Coordinators must be prepared to manage and respond to:

TYPE OF ATTACK	RISK - IMPACT	CONSEQUENCE
Phishing / Social Engineering	CRITICAL OR HIGH	Compromised user accounts; Loss of data or data exfiltrated from the university, university staff and students; Potential financial loss; Harm to FSU's reputation
Malware/ Ransomware / Wipers	CRITICAL OR HIGH	Data breach; Data loss
Password Attacks	MODERATE TO HIGH	Privilege escalation; Theft of sensitive information; Loss of use
Insider Threats	MODERATE TO HIGH	Loss of data; Loss of access to FSU's computing infrastructure; Violation of intellectual property rights
DoS / DDoS Attacks	MODERATE TO HIGH	Temporary outage; Performance degradation

1.2 CYBERSECURITY BEST PRACTICES

At all times, it is imperative to be prepared for disasters and worst-case scenarios. Below are some generally accepted practices and recommendations to review during times of potential increased cyberterrorism activity: [1]

- *The Multi-State Information Sharing and Analysis Center (MS-ISAC) recommends state and local governments and tribal territories (SLTT) remain vigilant of potential DDoS attacks and wipers as these are known tactics.*
- *Maintain log monitoring and heightened awareness for suspicious activity on networks, especially those related to critical infrastructure*
- *SLTT should evaluate third-party access to their networks and, if relevant, consider having a conversation with their third-party Managed Service Providers (MSPs) to ensure appropriate steps are taken to mitigate risk*
- *Evaluate and manage third-party risks from the supply chain, vendors, and vendor support personnel*
- *Keep all systems up-to-date and apply appropriate security patches when necessary*
- *Ensure backups of systems are current and stored offline*
- *Implement and maintained hardened configurations of systems*
- *All University colleges and departments must ensure they have current Information Technology Disaster Recovery Plans (ITDRP).*

All University technology professionals must review the recommendations above and ensure compliance during increased risk and ongoing acceptable standards.

Information Technology (IT) Security Incident Response and Reporting is tied to the principal university's 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.

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 reduces the university's impact from both financial and human resources (HR) perspectives.

[1] MS-ISAC Cyber Intel Advisory January 03, 2020 – IA2020-0101; Center for Internet Security, Department of Homeland Security

- 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 technology policies and standards requiring campus IT administrators to report and respond to IT security incidents. The following courses of action are required with the discovery of an IT security incident:

- The unit IT/Information Security Managers (ISMs) must immediately notify the FSU Chief Security Information Officer (CISO) of IT security incidents within their units, especially those threatening other IT resources (e.g., hacking of mail or webserver).
- In the event of a payment card data security breach, the department head must be notified immediately of any suspected or real security incidents involving computing assets, particularly any critical system. If it is unclear whether a situation should be considered a security incident, the department must coordinate with their departmental IT Security Manager to evaluate the situation. After the evaluation, the departmental IT Security Manager must escalate and notify the University Information Security Manager of the incident.
- The unit, IT/ISMs, must 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 a liaison during all IT security investigations (e.g., use of computing resources to commit credit card fraud).
- The FSU Office of General Counsel, CISO, 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 the existing internal capability to conduct computer analysis and related forensics, members of the FSU IT Security Incident Response Team (FSU CSIRT) 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 Cyber and Information Security and Privacy Process Description

2.1 Incident Identification

2.1.1 Overview

All students, faculty, and staff are responsible for remaining vigilant and protecting the data stored on systems we support. Any event that threatens the confidentiality, integrity, or availability of the information resources we support or utilize internally must immediately be reported to a manager or supervisor or the Information Security Manager (ISM) or Unit Privacy Coordinator (UPC) if a manager or supervisor is unavailable. Managers/Supervisors must immediately bring the incident to the university's Chief Information Security Officer (CISO).

Parents are encouraged to notify the university of possible breaches or improper disclosures of data using a form we have provided for this purpose.

2.1.2 Incident Types

Types of cyber and information security incidents that may threaten the organization are:

- Unauthorized attempts to gain access to a computer, system, or the data within
- Service disruption, including Denial of Service (DoS) attacks
- Unauthorized access to critical infrastructure, such as servers, routers, firewalls, etc.
- Virus or worm infection, spyware, or other types of malwares
- Non-compliance with security or privacy protocols
- Data theft, corruption, or unauthorized distribution

2.1.3 Incident Symptoms

Signs a computer system or network device may have been compromised include:

- Abnormal response time or non-responsiveness
- Unexplained lockouts, content or activity
- Locally hosted websites won't open or display inappropriate content or unauthorized changes
- Unexpected programs running
- Lack of disk space or memory
- Increased frequency of system crashes
- Settings changes
- Data appears missing or changed
- Unusual behavior or activity by staff, students, faculty, partners or other actors

2.2 Incident Assessment

2.2.1 Overview

Once the anomalous activity has been reported, it is incumbent upon the Department, Division, or Direct Support Organization Information Security Manager and Unit Privacy Coordinator to determine the required level of intervention. Other members of the CSIRT may be required to provide input during this phase to help determine if an actual security threat exists. If it is determined there is an active security threat or evidence of an earlier intrusion. In that case, the IRM will alert the entire CSIRT immediately so the situation may be dealt with as expeditiously as possible.

2.2.2 Considerations

- What are the symptoms?
- What may be the cause?
- What systems have been/are being/will be impacted?
- How widespread is it?
- Which stakeholders are affected?

2.2.3 Documentation

Regardless of whether it is determined there is a security threat, the IRM will accurately document the Cyber Security Incident scenario. All Cyber Security Incidents will be stored in a single location to review incident information in the future. This report should contain information such as:

- Who reported the incident?
- What are its Characteristics of the activity?
- Date and time the potential incident was detected.
- Nature of the incident (Unauthorized access, DDoS, Malicious Code, No Incident Occurred, etc.)
- Potential scope of impact.
- Is the CSIRT required to perform incident remediation?

2.3 Incident Reporting and Communications

2.3.1 Reporting Cybersecurity Incidents and Communication Guidelines

Cybersecurity Incident Reporting Procedures:

Departments will likely report cybersecurity incidents to ITS/Information Security and Privacy Office (ISPO) using one or more of the following options:

- Call the ITS Service Desk to verify if an email claiming to be from FSU is legitimate: 850-644-HELP (4357)
- Authenticated users can contact the FSU service center using the following link: https://servicecenter.fsu.edu/
- Unauthenticated FSU members can report via email, ITS Service Desk | Information Technology Services or chat https://messenger.providesupport.com/messenger/otc.html
- FSU members can find all these options on the https://its.fsu.edu/ website at the bottom under 'Contact Us'
- The FSU ISPO Security Operations Center (SOC) group monitors the Abuse@fsu.edu daily.

2.3.2 Information Security and Privacy Office Intelligence Services

The University Information Security Privacy Office (ISPO) receives and processes alerts from Multi-State - Information Sharing and Analysis Center (MS-ISAC), and Research Education Networking - Information Sharing and Analysis Center (REN-ISAC). These services monitor FSU's network 24 hours a day, seven days a week. Notifications are sent to ISPO SOC who coordinates with FSU departments to remediate the alerts. The MS-ISAC service also has probes around the U.S to determine if FSU accounts are compromised; FSU receives notifications daily. In addition, ISPO SOC subscribes to DORKBOT, which provides information related to web application servers that are compromised.
ISPO SOC also monitors the following intelligence feeds which are used to update FSU security members via Security@lists.fsu.edu:

- Homeland Security
- US Cert
- CI Security – Center for Internet Security
- MS-ISAC Advisory Alerts

For more detailed information related to Incident reporting, please refer to the following links:

4-OP-H-25.11 IT Incident Response Standard

Steps to Secure a compromised email:

https://its.fsu.edu/steps-secure-possibly-compromised-fsu-account

2.3.3 INCIDENT COMMUNICATION GUIDELINES

Communication with parents/community members will be coordinated through University Communications and the University Chief Information Officer and Chief Information Security Officer. All incident communications shall be disseminated consistent with applicable federal and state law and university official policies.

Although every incident is unique, sample communications that can be used as guidelines can be found in **Appendix B**.

Initial communication to affected stakeholders must occur as expeditiously as feasible upon identifying the incident and critical information or facts relating to the incident. In some instances, this may include an initial communication (letter, email, phone call) that simply states that the University [Department, Division, or Direct Support Organization] is aware of the issue and is working to address it the promise of a follow-up.

Unauthorized release of High Risk or Moderate Risk data, including Personally Identifiable Information (PII) as defined by 4-OP-H-25.01 Data Security Standard, must be addressed:

- Should the unauthorized release of High Risk or Moderate Risk student data occur, the university shall notify the parents (or eligible students) affected by the release in the most expedient way possible. University Policy requires this notification to occur within 3 business days after the breach is discovered.
- Should the unauthorized release of High Risk or Moderate Risk faculty, staff, alumni, student, or other data occur, the University [Department, Division, or Direct Support Organization] shall notify the University personnel or constituents affected by the release in the most expedient manner.
- Should the unauthorized release of other High Risk or Moderate Risk data occur, the head of the impacted Department, Division, or Direct Support Organization shall notify the University's Chief Information Security Officer (CISO) as soon as the unauthorized release is discovered.
- Should the unauthorized release of Social Security Numbers, Driver's License or Non-Driver ID Numbers, Passport Numbers, Account Numbers, or Credit/Debit Card numbers combined with PII occur, University [Departments, Divisions, or Direct Support University Units] should, where applicable, consult state and federal law to verify notification obligations.

Communication updates will come from the University Communications department and/or Chief Information Officer, Chief Information Security Officer, or the Incident Response Manager. As staff receive requests for information, they must pass those requests along to the Incident Response Manager and University Communications.

- University faculty and staff must be informed of what information is public and what is internal/confidential by their respective Department, Division, or Direct Support

Organization management team. *However, University leadership must be aware that any material or information communicated to faculty and staff can and likely will be shared with the public, including the news media.*

- Communication with news media or governmental entities will be initiated and coordinated through University Communications and ITS Communications teams.

  Incoming news media calls and requests for information will be directed through University Communications and the Incident Response Team working in conjunction with ITS Communications. A communication response plan (talking points, interview refusal statement, etc.) will be formulated as needed, with information coming from University Communications.

- University Communications will be responsible for disseminating information on University IT security incidents with the media. Please refer to any information requests concerning an IT security incident to this group as a single point of contact. Ensure your staff understand this procedure.
- When required, initial external/general communications messages must include broad language that offers basic information (1-2 sentences) and reassurance and refer to separate detailed communication pieces as a follow-up activity, when additional facts relevant to the incident have been ascertained.

2.4 Incident Response

2.4.1 Briefing of Administration

Upon determining that a significant incident or breach has occurred, University Leadership must be notified immediately. As additional information is uncovered throughout the investigation, leadership must be briefed by the Chief Information Officer and Chief Information Security Officer, so appropriate decisions, such as allocating additional staff, hiring outside consultants, and involving law enforcement, can be made.

Additionally, based on the incident, it will be incumbent on leadership to determine the appropriate stakeholders to notify the incident and the appropriate medium. Notification requirements must consider the nature of the information or systems involved, the scope of the party's affected timeliness, potential law enforcement interests, applicable laws, and the communication requirements of all parties involved. Sample communications documents are provided for this purpose.

2.4.2 Initial Response

The first steps in any cyber incident response should be to determine the origin of the incident, isolate the issue, and contain the impact. The response may involve measures up to and including disconnecting workstations, servers, or network devices from the network to prevent additional loss. While this is occurring, it is necessary to examine firewall and system logs and

possibly perform vulnerability scans to ensure the incident has not spread to other areas to define the incident's entire scope.

It will be critical to preserve all possible evidence throughout this process and document all measures taken in detail. A thorough review is required once the threat has been removed, the vulnerabilities patched, and the systems have been restored.

2.4.3 Remediation and Recovery

Once the cause has been determined and appropriately isolated, the CSIRT will need to remove the vulnerabilities leading to the incident. Remediation may involve some or all the following:

- Install security patches and software updates on systems, routers, and firewalls
- Infections cleaned and removed
- Re-image or re-install operating systems of infected machines
- Change appropriate passwords
- Conduct a vulnerability scan of any compromised devices before reconnecting them to the network
- Restore system backups where possible
- Document all recovery procedures performed and submit them to the IRM
- Closely monitor the systems once reconnected to the network

2.5 Incident Report

2.5.1 Overview

Once the threat has been mitigated, and normal operation is restored, the Information Security Manager (ISM) and Unit Privacy Coordinator (UPC) will compile all available information to produce an accurate and in-depth summary of the incident using an Incident Summary Report (ISR). Throughout the incident, the CSIRT will have kept Incident Logs that contain detailed records wherever possible, and these shall serve as the basis of the report. Interviews will also be conducted with appropriate members of the CSIRT to obtain any additional information that may be available to augment the logs and records kept throughout the process.

2.5.2 Incident Report Contents

The Incident Summary Report (ISR) will include all pertinent information describing the incident, including the items specified below:

- Dates and times of milestones throughout the process (e.g., incident detection, verification, notifications, remediation steps, completion, etc.)
- List of symptoms or events leading to the discovery of the incident
- Scope of impact
- Mitigation and preventative measures
- Restoration logs
- Key Stakeholder communications (including copies of memos, emails, etc. where possible)

2.5.3 TIMEFRAME

The ISR should be prepared as expeditiously as possible following the incident so future preventative measures may be taken as quickly as possible. Information to prepare the ISR and interviews with the CSIRT should be conducted immediately to ensure information accuracy.

2.6 INCIDENT AFTER ACTION REVIEW

2.6.1 POST-INCIDENT / AFTER ACTION REVIEW MEETING

After the conclusion of the incident, the IRM and possibly select members from the CSIRT will meet with management to discuss the event in detail, review response procedures, and construct a Process Improvement Plan (PIP) to prevent a recurrence of that or similar incidents. The compiled Incident Report constructed by the IRM will serve as a guide for this meeting.

In the meeting, a full debrief of the incident will be presented, and the findings discussed. The IRM will share the full scope of the breach (as comprehensively as possible), causes of the breach, how it was discovered, potential vulnerabilities that still exist, communication gaps, technical and procedural recommendations, and the overall effectiveness of the response plan.

The group will review the information presented. It will determine any weakness in the process, select the appropriate actions to modify the plan, address any vulnerabilities, and what communication is required to various stakeholders.

2.6.2 PROCESS IMPROVEMENT PLAN

The IRM will draft a Process Improvement Plan (PIP) based on the results of this meeting. The plan should discuss any applicable items necessary to prevent future incidents to an extent practicable, including cost and time frame requirements where possible. The PIP will also include a review strategy to ensure all PIP recommendations are met in a timely fashion and function appropriately. Areas of focus may include, but are not limited to:

- New hardware or software required

- Patch or upgrade plans
- Training plans (Technical, end-users, etc.)
- Policy or procedural change recommendations
- Recommendations for changes to the Incident Response Plan
- Regional communications recommendations

Additionally, the PIP must be kept strictly confidential for security purposes. Any communication required by clients, or the public, must be drafted separately and include only the necessary information to prevent future incidents.

3.0 Reporting and Responding to Cyber or Information Security Incidents

3.1 Reporting of Cyber and Information Security Incidents

There are many diverse kinds of IT Security Incidents, and various 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 shall be reported to the FSUPD. Employee misconduct, both criminal and otherwise, shall also be reported to Human Resources. Incidents of a technical nature usually deriving from an external source must be reported to the CISO.

University data owners are responsible for ensuring the information and data we are entrusted with managing is classified according to requirements established in 4-OP-H-25.01 Data Security Standard.

All University data, irrespective of the format or medium of the record, i.e., paper, electronic media containing data, audio, voice recordings, video or images, microfilm, etc., are required to be classified into one of three sensitivity levels as High Risk, Moderate Risk, or Low Risk data. .

- **High Risk Data - severe or catastrophic adverse effects could be expected**
  Data that is collected, developed, maintained, or managed by or on behalf of FSU and is protected by law, contracts, university patents or to mitigate institutional risks is defined as High Risk. Any information that could, if exposed, create civil or criminal penalties, reputational damage, or loss of protected intellectual property is also classified as High Risk. Examples include Personally Identifiable Information (PII), Student Information (FERPA), Credit Card information, some research information, etc.
- **Moderate Risk Data - serious adverse effects could be expected**
  Data that is not specifically protected by legal or contractual mandates but for which unauthorized access or modification could cause financial loss, damage to FSU's

reputation, violate an individual's privacy rights, or make legal action necessary. Examples include name in combination with other personal information, course evaluations, etc.

- **Low – limited adverse effects could be expected**
  Data that is not classified as High or Moderate Risk that is designated as publicly available, without requiring the specific information custodian's approval. Low Risk data does not expose FSU to financial loss or jeopardize the security of IT Assets or physical security. Examples include public facing websites, unrestricted research data, etc.

The data classification level associated with an incident is an essential component in timely risk mitigation in the response process.

Cybersecurity Incident Reporting Procedures:

Departments are responsible for reporting incidents to ITS/ISPO using one or more of the following options:

- Call the ITS Service Desk to verify if an email claiming to be from FSU is legitimate: 850-644-HELP (4357)
- Authenticated users can contact the FSU service center using the following link: https://servicecenter.fsu.edu/
- Unauthenticated FSU members can report via email its-servicedesk@fsu.edu, or chat https://messenger.providesupport.com/messenger/otc.html
- FSU members can find all these options on the https://its.fsu.edu/ website at the bottom under 'Contact Us'
- The FSU Information Security and Privacy Office Security Operations Center (SOC) group monitors the Abuse@fsu.edu daily.

3.1.1 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 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

3.1.2 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 described in 4-OP-H-21 Acceptable Use of Technology Policy 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 employees' jobs
4. Use of IT resources that result in unapproved costs to the University

3.1.3 Types of IT Security Incidents Reported to CJIS (Criminal Justice Information Systems) 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 CJIS system user 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, LASO or TAC is responsible for ensuring the FDLE Information Security Officer (ISO) is immediately notified.
5. LASO is responsible for collecting and logging information concerning the incident.

3.1.4 Types of Major Cyber or Information Security Incidents Reported to ISPO

1. Unauthorized disclosure of Personally Identifiable Information (PII), Protected Health Information (PHI). The University is required to investigate any incident that may involve the breach of personally identifiable information by various Florida Statutes, e.g., *s. 501.171, F.S.*, federal law, *e.g., Family Educational Rights and Privacy Act (FERPA), Health Information Portability and Accountability Act (HIPAA), and Graham Leach Bliley (GLB), etc.*, and contractual obligations, *such as those defined in the Payment Card Industry Data Security Standard (PCI DSS*.
2. The university may also be required to notify an individual if the privacy of a combination of public and PII data has been compromised. The dean, director, or department head of the University entity 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, the Chief Information Security Officer, and the Chief Information Officer.

3. Root or system-level attacks on mission-critical applications or information systems, desktops, laptops, smartphones, tablets, servers, firewalls, storage devices, etc., or on any part of the supporting University voice or data network infrastructure, e.g., switches, wireless access points, routers, etc. can be especially harmful.
4. Unauthorized root or privileged access to a computing or storage device may allow the user to read, write, and update capabilities over data, applications, and the device's configuration and security settings.
5. Unauthorized root access on a network data or voice communications device may allow the intruder the ability to intercept encrypted or unencrypted communications, reroute network traffic to unintended devices, change device security settings, or conduct denial of service attacks.
6. Root or system-level attacks on any FSU computing device that the authorized user may use to conduct University business with data classified as High Risk or Moderate Risk information or authenticate into critical University systems and store data on the device.
7. Compromise restricted protected service accounts or software installations, particularly those used for IT applications containing data classified as High Risk or Moderate Risk, or those used for system administration.
8. Denial of service attacks that impair the availability of FSU computing resources.
9. Malicious code attacks, including malware infections on devices, may allow unauthorized users to bypass system security controls on systems accessing, transmitting, or storing data classified as High Risk or Moderate Risk. Also, vulnerabilities in application code may be used to bypass security controls to change application security settings, access supporting database(s) storing High Risk or Moderate Risk data, or reroute users to an unauthorized site.
10. Open mail relay is used to forward spam or other unauthorized communications associated with a university email account.
11. 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, Canvas, OMNI, Campus Solutions, NWRDC mainframe applications, and Email accounts.
12. Denial of service on individual user accounts
13. Any other 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.

3.1.5 TYPES OF MINOR SECURITY INCIDENTS

Virus infections on servers and endpoints that do not contain data classified as High Risk or Moderate Risk or are not used to process High Risk or Moderate Risk data in a public location such as a kiosk.

3.2 Departmental Response to IT Security Incidents

3.2.1 Isolation and Protection of Compromised Device(s)

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

1. Discontinue use of that device immediately.
2. Do not power off the device; this could delete useful information for an investigation.
3. Disconnect the network cable at the network jack in the wall or switch.
4. Isolate the computer to prevent any further use.
5. Preserve logs on any devices in the system or network to aid in forensic analysis.
6. Depending on the type of suspected compromise, contact the FSUPD, HR, or the FSU IT Security Incident Officer to assist in the investigation. If necessary, get a backup of the hard drive.

3.2.2 Identification of Personally Identifiable Data

Analyzing what data and applications might have been potentially exposed is an essential 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.

3.2.3 Calculation of Campus Unit Fiscal Cost to Remediate Incident

It is the university's responsibility 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 on 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 re-imaging or a forensic examination.

4. Record any third-party costs if outside entities are contracted to assist in forensic or technical assistance during remediation.

   Appendix B contains an example of a master worksheet that can be used to estimate response costs. Each campus unit will maintain a subsidiary worksheet similar to the master worksheet for submission to ISPO after completing the remediation effort.

4.0 RESPONSIBILITIES OF FSU CSIRT (FSU CYBER AND INFORMATION SECURITY INCIDENT RESPONSE TEAM)

Creating an interdisciplinary Cyber and Information Security incident response team (CSIRT) drawn from all parts of the university and is trained to respond to events is vital to a comprehensive IT Security incident response program. The FSU CSIRT is directly responsible for providing information and assistance to the university community members when responding to incidents.

Each incident could require various FSU constituents and personnel to be available for investigation and remediation. In coordination with the CIO, the CISO will select from the organizational units deemed technically proficient at providing their expertise to the particular incident. The following University administrative units may be convened depending on the incident reported.

Function/Incident Type	Campus Unit
Direction and oversight for IT issues	CIO and ITS
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
HIPAA data incident	Local HIPAA Privacy Officer
Windows and Virtual Machine supported data environment	ITS Infrastructure and Operations
Unix/Linux supported environments	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 environments	Department System Administrators
Public communications and responses to press inquires	University Communications and ITS Communications Teams
Regulation and policy expertise	Inspector General, General Counsel, ITS, Information Security and Privacy Office

The FSU CSIRT 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. Violations to acceptable use are defined in FSU Policy 4-OP-H-21 Acceptable Use of Technology Policy.

The FSU CSIRT is authorized to address all types of computer security incidents that might occur at FSU. Incidence response actions will be prioritized based on the following relevant considerations.

- **Functional impact** – Determination of the Scope of Negative Impact on University functions
- **Information or Data impact** – Understanding of the impact on the confidentiality, integrity, and availability of information and data
- **Recoverability Impact** – Understanding the requirements associated with restoration and recovery, including the resources and time allocated to manage, respond to, and recover from the incident.

The Florida State University Police Department (FSUPD) will act as a liaison for any incident/event requiring contact with outside law enforcement agencies to ensure the proper agencies are notified and integrated into university incident response activities.

4.1 Cyber and Information Security Incident Debriefing

4.1.1 After Action Analysis and Lessons Learned

One of the essential parts of incident response is also the most often omitted: learning and improving after a significant incident.

Each incident response team should evolve and enhance its capabilities to reflect new threats, improved technology, and lessons learned. Holding an after-action analysis or "lessons-learned" meeting with all parties involved 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 for an incident by reviewing what occurred, what was done to intervene, and how well intervention worked. The discussion should be held within several days of the end of the incident.

Key Information and questions to be addressed during the meeting include:

- Precisely 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 effective?
- 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 University Units have been improved?
- What if any corrective actions can prevent or reduce the impact of similar incidents in the future?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

4.1.2 Cyber and Information Security Major Incident Report Creation and Distribution

The FSU CSIRT, involved in the remediation of an incident classified as a major event, will create a report after completing the incident after-action analysis.

The report will be available to the campus unit administrator, dean, director, or department head at the discretion of the CISO or University Chief Information Officer.

APPENDIX A – SECURITY INCIDENT RUNBOOKS

MALWARE/MALICIOUS CODE/SPYWARE - A program inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of data, applications, or operating system or of otherwise annoying or disrupting the victim. A compromise can be in the form of a virus, worm, Trojan, or a backdoor (which can give an attacker access to a compromised system around any security mechanism).

PHISHING/SOCIAL MEDIA - An attempt to trick someone into clicking on a link to install ransomware or other programs that can lock you out of your data and spread laterally on the network to other systems or to reveal information (e.g. a password) that can be used to attack systems or networks.

COMPROMISED CREDENTIALS - The unauthorized disclosure of a password, token, or other user credentials can provide access to organizational systems or data. The credential may become compromised through various means, such as phishing, malware, social engineering, or accidental means.

DEFACEMENT/WEBSITE SECURITY - An attack involving the modification of a website's content in such a way that it becomes "vandalized" or embarrassing to the website owner.

DATA BREACH (UNAUTHORIZED DISCLOSURE OF HIGH RISK/MODERAT RISK INFORMATION) - The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information. A data breach can include business information (such as trade secrets, financial data, acquisition plans), personal identifiable information, or personal health information.

DENIAL OF SERVICE (DoS)/ DISTRIBUTED DENIAL OF SERVICE (DDoS) - An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim of or participating in a DoS, or the use of a botnet to prevent authorized access to a system resource or the delay of system operations and functions. A botnet uses many compromised computers to create and send spam or viruses or flood a network with messages as a denial-of-service attack.

SECURITY INCIDENT CATEGORY: MALWARE / MALICIOUS CODE / SPYWARE

COORDINATING UNITS

UNIT		Name	Phone	EMAIL
ISPO	Information Security and Privacy Office	Bill Hunkapiller Tom Doughty Clifford Stokes Joe Thomas	850-645-0676 850-363-5041 850-339-5900 407-334-9020	bill.hunkapiller@fsu.edu tdoughty@fsu.edu cstokes3@fsu.edu joe.thomas@fsu.edu
NCT	Network Communication Technologies	Jason Grimes	850-645-3531	jegrimes@fsu.edu
CTS	Computer Technical Support	Alex Morales Andrew Kocur Jason Penley Claire Borschel	850-644-4883 850-644-8088 850-644-8088 850-644-8088	amorales@fsu.edu akocur@fsu.edu jpenley@fsu.edu cborschel@fsu.edu
LEAS	Infrastructure Services	Breeze Howard	850-645-8008	bhoward@fsu.edu
MEAS	Collaboration Services	Corey Webster	850-644-7758	cmwebster@fsu.edu
WS	Web Services	Debbie Kelly	850-645-8012	kelly@fsu.edu
ESVS	Platform Administration	Johnny White	850-645-8011	jcwhite3@fsu.edu
IAM	Identity and Access Management	Martin Schaefer	304-523-3286	MSchaefer@admin.fsu.edu
SD	Service Desk	Lisa Martin-Brown	850-645-7935	Lmartinbrown@fsu.edu

PREPAREDNESS

In the FSU environment, Windows Defender Antivirus delivers comprehensive, ongoing, and real-time protection against software threats like viruses, malware, and spyware across email, apps, cloud, and the web.

The Palo Alto Networks PA-5445 Next Generation Firewall provides industry-leading threat effectiveness against both known and unknown threats. Features include:

- IPS rules that identify and block attack traffic that target network vulnerabilities.
- Tightly integrated defense against advanced malware incorporating advanced analysis of network and end-point activity.
- Sandboxing technology uses hundreds of behavioral indicators to identify zero-day and evasive attacks.

Cisco Umbrella prevents command and control attacks. When a user on your network sends a request to the internet, Umbrella compares the requested domain to their directory of suspicious domains. If the domain is malicious, the traffic is immediately blocked, including command and control sites.

DorkBot notifies ITS of compromised Web servers.

MS_ISAC notifies ITS of compromised accounts or accounts being used to spread phishing attacks.

SCCM System Center Configuration Manager. Allows ITS CTS to remediate issues with endpoints. Insight VM and CrowdStrike Vulnerability Management allows ITS staff to determine if endpoints and servers are susceptible to an attack.

Network segmentation involves splitting the larger network into smaller network segments using firewalls, virtual local area networks (VLANs), and other separation techniques. Segmentation lays the groundwork for controls that protect against lateral movement on the network by ransomware or hackers, preventing an infection or compromise from spreading across the network.

RESPONSE

- Determine the type of exploit and what systems are involved.
- Coordinate with ITS and Campus IT staff to notify the responsible unit they have a compromised device or account.
- Coordinate with ITS-Core if ports/VLANs/VRFs need to be quarantined.
- Work with the affected unit to scan or re-image the device.
- Conduct a debrief to determine if High Risk or Moderate Risk Data was lost/exfiltrated, the root cause, and document actions taken.
- Create an incident report.
- Document according to CSIRT procedure.

SECURITY INCIDENT CATEGORY: PHISHING/SOCIAL MEDIA

COORDINATING UNITS

UNIT		Name	Phone	EMAIL
ISPO	Information Security and Privacy Office	Bill Hunkapiller Tom Doughty Clifford Stokes Joe Thomas	850-645-0676 850-363-5041 850-339-5900 850-645-8055	bill.hunkapiller@fsu.edu tdoughty@fsu.edu cstokes3@fsu.edu joe.thomas@fsu.edu
NCT	Network Communication Technologies	Jason Grimes	850-645-3531	jegrimes@fsu.edu
CTS	Computer Technical Support	Alex Morales Andrew Kocur Jason Penley Claire Borschel	850-644-4883 850-644-8088 850-644-8088 850-644-8088	amorales@fsu.edu akocur@fsu.edu jpenley@fsu.edu cborschel@fsu.edu
LEAS	Infrastructure Services	Breeze Howard	850-645-8008	bhoward@fsu.edu
MEAS	Collaboration Services	Corey Webster	850-644-7758	cmwebster@fsu.edu
WS	Web Services	Debbie Kelly	850-645-8012	kelly@fsu.edu
ESVS	Platform Administration	Johnny White	850-645-8011	jcwhite3@fsu.edu
IAM	Identity and Access Management	Martin Schaefer	304-523-3286	MSchaefer@admin.fsu.edu
SD	Service Desk	Lisa Martin-Brown	850-644-3231	Lmartinbrown@fsu.edu

PREPAREDNESS

ISPO conducts phishing awareness training on an ongoing basis. ISPO also maintains a web page dedicated to phishing, which includes the phish tank, which provides examples of Phishing attempts sent to us by FSU students and staff.

MS Proofpoint is used to detect and block sites known to engage in social engineering.

RESPONSE

- Identify who was affected (Splunk, Proofpoint dashboard, Azure tools).
- Identify the type of compromise (Financial Gain, Stolen Credentials).
- Determine how to remediate (Block User, Reset Passwords for those affected).
- Create an incident report.
- Document according to CSIRT procedure.

SECURITY INCIDENT CATEGORY: COMPROMISED CREDENTIALS

COORDINATING UNITS

UNIT		Name	Phone	EMAIL
ISPO	Information Security and Privacy Office	Bill Hunkapiller Tom Doughty Clifford Stokes Joe Thomas	850-645-0676 850-363-5041 850-339-5900 850-645-8055	bill.hunkapiller@fsu.edu tdoughty@fsu.edu cstokes3@fsu.edu joe.thomas@fsu.edu
NCT	Network Communication Technologies	Jason Grimes	850-645-3531	jegrimes@fsu.edu
CTS	Computer Technical Support	Alex Morales Andrew Kocur Jason Penley Claire Borschel	850-644-4883 850-644-8088 850-644-8088 850-644-8088	amorales@fsu.edu akocur@fsu.edu jpenley@fsu.edu cborschel@fsu.edu
LEAS	Infrastructure Services	Breeze Howard	850-645-8008	bhoward@fsu.edu
MEAS	Collaboration Services	Corey Webster	850-644-7758	cmwebster@fsu.edu
WS	Web Services	Debbie Kelly	850-645-8012	kelly@fsu.edu
ESVS	Platform Administration	Johnny White	850-645-8011	jcwhite3@fsu.edu
IAM	Identity and Access Management	Martin Schaefer	304-523-3286	MSchaefer@admin.fsu.edu
SD	Service Desk	Lisa Martin-Brown	850-644-3231	Lmartinbrown@fsu.edu

PREPAREDNESS

Implement multi-factor authentication (MFA).

Institute the policy of least-privilege.

Implement privileged session management.

Enforce strong passwords.

Monitor login activity for anomalies, such as concurrent logins, logins from new devices, IPs or locations, or logins from remote locations.

RESPONSE

- Immediately lock the user's account.
- Change the user's password to a new value, which should be considered temporary.
- Transmit the user's new password in a safe manner (email is not considered safe).
- For sensitive applications, university staff must check application activity logs to see whether any login has taken place after the user reported their credentials to be compromised.
- If there is evidence of unauthorized logins, the IT service desk must declare a security incident and notify appropriate personnel.
- Determine if other accounts used by the same person may be compromised.
- If the organization experiences a compromise of one or more privileged accounts. The university needs to take the same steps as listed above and closely monitor activity on privileged accounts. In that case, to ensure that all activities are authorized.

In relationships with third parties, this can become much more complicated. There are several considerations for University Units with third-party personnel who have privileged access to one or more of the organization's critical systems:

- Vendor agreements must include language whereby the third-party vendor agrees to comply with all applicable FSU policies and standards, and all agreed-upon applicable and appropriate security terms and conditions, as defined by 4-OP-H-25.13 IT Third-Party Vendor Management Standard.
- University Units may want to contractually require critical third parties to issue alerts when privileged credentials on affected systems are compromised.
- University Units may want to contractually require that critical third parties implement security controls such as advanced malware prevention, intrusion prevention systems (IPS), and user behavior analytics (UBA) to protect third-party organization endpoints, particularly for any personnel who have privileged access into critical systems.
- University Units that issue privileged credentials in their critical systems to any third-party personnel may need additional controls to ensure that credentials are always safe.
- Implement multi-factor authentication.
- Create an incident report.
- Document according to CSIRT procedure.

SECURITY INCIDENT CATEGORY: DEFACEMENT / WEBSITE SECURITY

COORDINATING UNITS

UNIT		Name	Phone	EMAIL
ISPO	Information Security and Privacy Office	Bill Hunkapiller Tom Doughty Clifford Stokes Joe Thomas	850-645-0676 850-363-5041 850-339-5900 850-645-8055	bill.hunkapiller@fsu.edu tdoughty@fsu.edu cstokes3@fsu.edu joe.thomas@fsu.edu
NCT	Network Communication Technologies	Jason Grimes	850-645-3531	jegrimes@fsu.edu
CTS	Computer Technical Support	Alex Morales Andrew Kocur Jason Penley Claire Borschel	850-644-4883 850-644-8088 850-644-8088 850-644-8088	amorales@fsu.edu akocur@fsu.edu jpenley@fsu.edu cborschel@fsu.edu
LEAS	Infrastructure Services	Breeze Howard	850-645-8008	bhoward@fsu.edu
MEAS	Collaboration Services	Corey Webster	850-644-7758	cmwebster@fsu.edu
WS	Web Services	Debbie Kelly	850-645-8012	kelly@fsu.edu
ESVS	Platform Administration	Johnny White	850-645-8011	jcwhite3@fsu.edu
IAM	Identity and Access Management	Martin Schaefer	304-523-3286	MSchaefer@admin.fsu.edu
SD	Service Desk	Lisa Martin-Brown	850-644-3231	Lmartinbrown@fsu.edu

PREPAREDNESS

Review registrar and domain name system (DNS) records periodically.

Enforce multi-factor (MFA) authentication.

Do not use default passwords on systems/servers.

Utilization of DorkBot alerts to notify ITS of compromised Web servers – REMEDIATE VULNERABILITIES.

Periodically scan web services using Insight VM or CrowdStrike Vulnerability Management to determine if endpoints and servers are susceptible to an attack - REMEDIATE VULNERABILITIES.

Disable HTTP and enforce HTTPS (Secure data in transit).

Backup data.

RESPONSE

Identify web service owners.
Restore the system from a backup.
Ensure the following:

- Sanitization of user input
- Optimized resource availability
- Implement cross-site scripting (XSS) and cross-site request forgery (XSRF) protections
- Implement a content security policy (CSP)

- Audit third-party code
- Deploy a web application firewall
- Create an incident report. Document according to CSIRT procedure.

SECURITY INCIDENT CATEGORY: DATA BREACH

COORDINATING UNITS

UNIT		Name	Phone	EMAIL
ISPO	Information Security and Privacy Office	Bill Hunkapiller Tom Doughty Clifford Stokes Joe Thomas	850-645-0676 850-363-5041 850-339-5900 407-334-9020	bill.hunkapiller@fsu.edu tdoughty@fsu.edu cstokes3@fsu.edu joe.thomas@fsu.edu
NCT	Network Communication Technologies	Jason Grimes	850-645-3531	jegrimes@fsu.edu
CTS	Computer Technical Support	Alex Morales Andrew Kocur Jason Penley Claire Borschel	850-644-4883 850-644-8088 850-644-8088 850-644-8088	amorales@fsu.edu akocur@fsu.edu jpenley@fsu.edu cborschel@fsu.edu
LEAS	Infrastructure Services	Breeze Howard	850-645-8008	bhoward@fsu.edu
MEAS	Collaboration Services	Corey Webster	850-644-7758	cmwebster@fsu.edu
WS	Web Services	Debbie Kelly	850-645-8012	kelly@fsu.edu
ESVS	Platform Administration	Johnny White	850-645-8011	jcwhite3@fsu.edu
IAM	Identity and Access Management	Martin Schaefer	304-523-3286	MSchaefer@admin.fsu.edu
SD	Service Desk	Lisa Martin-Brown	850-644-3231	Lmartinbrown@fsu.edu

PREPAREDNESS

Work with employees to integrate data security efforts into their daily work habits.
Ensure all units perform data classification, and all users are trained to handle data based on their respective classification.

Develop data security and mobile device policies, update them regularly, and communicate them to business associates.

Invest in proper cybersecurity software, encryption devices, and firewall protection. Update these security measures regularly.

Limit the type of both hard and electronic data someone can access based on the job.
Conduct employee security training/re-training at least once a year.

RESPONSE

Record the date and time when the breach was discovered, as well as the current date and time when response efforts begin, i.e., when someone on the response team is alerted to the breach.

Alert and activate everyone on the FSU CSIRT response team.
Secure the premises around the area where the data breach occurred to help preserve evidence.

Stop additional data loss. Take affected machines offline (unplug from the network) but do not turn them off or start probing into the computer until forensics can be performed.

Document everything known about the breach: Who discovered it, who reported it, to who it was reported, who else knows about it, what type of breach occurred, what was stolen; How was it stolen, what systems are affected, what devices are missing, etc. Interview those involved in discovering the breach and anyone else who may know about it.

Review protocols regarding disseminating information about the breach for everyone involved in this early stage.

Notify law enforcement, if needed, after consulting with legal counsel and upper management. Create an incident report.

Document according to CSIRT procedure.

SECURITY INCIDENT CATEGORY: DENIAL OF SERVICE / DISTRIBUTED DENIAL OF SERVICE

COORDINATING UNITS

UNIT		Name	Phone	EMAIL
ISPO	Information Security and Privacy Office	Bill Hunkapiller Tom Doughty Clifford Stokes Joe Thomas	850-645-0676 850-363-5041 850-339-5900 850-645-8055	bill.hunkapiller@fsu.edu tdoughty@fsu.edu cstokes3@fsu.edu joe.thomas@fsu.edu
NCT	Network Communication Technologies	Jason Grimes	850-645-3531	jegrimes@fsu.edu
CTS	Computer Technical Support	Alex Morales Andrew Kocur Jason Penley Claire Borschel	850-644-4883 850-644-8088 850-644-8088 850-644-8088	amorales@fsu.edu akocur@fsu.edu jpenley@fsu.edu cborschel@fsu.edu
LEAS	Infrastructure Services	Breeze Howard	850-645-8008	bhoward@fsu.edu
MEAS	Collaboration Services	Corey Webster	850-644-7758	cmwebster@fsu.edu
WS	Web Services	Debbie Kelly	850-645-8012	kelly@fsu.edu
ESVS	Platform Administration	Johnny White	850-645-8011	jcwhite3@fsu.edu
IAM	Identity and Access Management	Martin Schaefer	304-523-3286	MSchaefer@admin.fsu.edu
SD	Service Desk	Lisa Martin-Brown	850-644-3231	Lmartinbrown@fsu.edu
FLR	Florida Lambda Rail (ISP)	CTS	CTS	CTS

PREPAREDNESS

The Palo Alto Networks PA-5445 Next Generation Firewall provides industry-leading threat defense against both known and unknown threats. Features include:

- IPS rules that identify and block attack traffic that target network vulnerabilities
- Tightly integrated defense against advanced malware incorporating advanced analysis of network and end-point activity
- Sandboxing technology that uses hundreds of behavioral indicators to identify zero-day and evasive attacks

Florida Lambda Rail (FLR) – upstream internet service provider (with their DDoS mitigation service).

ACLs applied on border routers - used to block known malicious IP prefixes.

RESPONSE

Identify the Source and Target IP Address Range(s), Ports, and Protocols.

Identify ownership of Source IP addresses.

Decide if action needs to be taken.

If we elect to block,

Aggregate IP range (if necessary) and deny attacking source IP range.

Determine where to block (IPS, BR, or FLR).

Apply ACL.

Create an incident report.

Document according to CSIRT procedure.

SECURITY INCIDENT CATEGORY: FERPA INCIDENTS

HANDLING OF FERPA INCIDENTS

FERPA is a federal law that is administered by the Student Privacy Policy Office (Office) in the U.S. Department of Education (Department). 20 U.S.C. § 1232g; 34 CFR Part 99. FERPA applies to all educational agencies and institutions that receive funding under any program administered by the Department.

While FERPA does not contain specific breach notification requirements when information is compromised, it protects the confidentiality of education records by requiring a record of each incidence of data disclosure. Additionally, other state and federal laws may require breach notification even if FERPA does not.

Upon discovery of an actual or potential FERPA incident in which information may have been compromised, the department that maintained the information at the time of the incident will report the incident by emailing privacyincident@fsu.edu as soon as possible after discovery. As each FERPA incident could require various FSU constituents and personnel to be available for investigation and remediation, the CISO in coordination with the CIO will select from the organizational units deemed technically proficient to provide their expertise to the FERPA incident.

ITS is responsible for helping to determine the potential for harm resulting from the compromise of the information and assisting with ensuring compliance with FERPA and other laws protecting confidential personal information.

ITS staff will determine whether notification is warranted and, if so, to whom and when the notification must be made. Executive leadership at the senior technical and/or administrative level, in coordination with the Offices of the General Counsel and Compliance and Ethics, is the authority that must make this decision.

Upon determination that a notification is warranted, the department that maintained the information at the time of the incident will notify affected individuals whose sensitive information, including PII, has been compromised. Such notification must comply with the minimum notification requirements established by applicable federal, state, and local laws.

If current student notification is deemed necessary, email correspondence must be provided to the student including detailed information regarding the incident, if there is any potential future harm due to the nature of the information compromised, steps taken to mitigate the breach, as well as a contact email if the student has any additional questions regarding the incident. If an incident affects former student information and a notification is deemed necessary, notification will be sent via mail correspondence to the permanent physical address on record with the university. Notifications must be provided in a straightforward and honest manner, ensuring thorough and complete notification to the best of staff ability.

Upon receipt of a question or response from a student based on a FERPA breach notification, it is important that staff acknowledge receipt of the student's email. The following response must be sent in response via email once email is received:

"Thank you for contacting the Information Security and Privacy Office (ISPO). This email serves as confirmation that your email has been received. A member of the ISPO team will respond as quickly as possible. Please note responses will be handled during normal business hours, those requests sent outside of these hours may result in a delayed response time. Thank you and have a wonderful day."

Prompt response is essential for minimizing the risk of any further data loss and, therefore, plays an important role in mitigating any negative consequences of the breach, including potential harm to affected individuals. All FERPA incident response activities will be documented to include artifacts obtained using methods consistent with chain of custody and confidentiality requirements. Documentation is sufficient to support the declaration, remediation, and recovery from the incident. Incidents will be prioritized and ranked according to their potential risk. As an investigation progresses, that ranking may change, resulting in a greater or lesser prioritization of ISPO resources.

Appendix B – Incident Communication Templates

Parent or Guardian Template

DATE

Dear **[Parents/Guardians]**,

This letter is to inform you of an incident that occurred within the **XXXXXXX**. This incident resulted in **student/faculty/staff/etc.** data being compromised by an outside entity. Our Incident Response Team acted quickly to assess and mitigate the situation.

At this time, we can share the following details:

[Insert a brief description of the breach or unauthorized release, the dates of the incident and the date of discovery; a description of the types of personally identifiable information affected; an estimate of the number of records affected; a brief description of the educational agency's investigation or plan to investigate]

Please know that **XXXXXXX** is committed to protecting and securing educational data. Our team has extensive training in data security and privacy, and our systems have many controls in place to protect your child's academic records. Our team is working with a group of experts to review the incident and implement appropriate measures to protect against this type of incident from occurring in the future.

Please contact **XXXXXXX** with any questions you may have regarding this incident and our response.

Sincerely,

FACULTY/STAFF TEMPLATE

DATE

Dear **[Faculty or Staff]**,

This letter is to inform you of an incident that occurred on **DATE** within the **XXXXXXX**'s **YYYYYYY** system. This incident resulted in **student/faculty/staff/etc.** data being compromised by an outside entity. Our response team acted quickly to assess and mitigate the situation.

I wanted to ensure that you have key details of the incident, so you are well-informed when speaking with your students and colleagues. Please note that **XXXXXXX** administration is handling communication with the community and affected parties. Should you receive any related inquiries, please direct them to **XXXXXXX.**

At this time, we can share the following details:

[Insert a brief description of the breach or unauthorized release, the dates of the incident and the date of discovery; a description of the types of personally identifiable information affected; an estimate of the number of records affected; a brief description of the educational agency's investigation or plan to investigate]

As more details become available, we will be disseminated as appropriate.

Please contact **XXXXXXX** should you have any questions or immediate concerns regarding this incident.

Sincerely,

EXTERNAL COMMUNICATION TEMPLATE

The university **[department, division, DSO]** experienced a technical issue today with its **YYYYYYY** system that may have resulted in **[student/faculty/staff/etc.]** data being compromised. The issue is currently under investigation. More detailed information will be distributed shortly via **ZZZZZZZ**.

External Source of Unauthorized Disclosure Form

Parents, eligible students (students who are at least 18 years of age or attending the university at any age), faculty, staff, and employees of the university may file a complaint about a possible breach or improper disclosure of student data or protected data using this form.

A privacy complaint may be made using this online form or by mailing the form to the University **[Insert point of contact] at [Insert University Department address]**.

CONTACT INFORMATION

First Name: Last Name:
Phone Number: Email:
Role:

IMPROPER DISCLOSURE OR BREACH INFORMATION

Date of Unauthorized Disclosure:
Description of Data Compromised:
Description of Improper Disclosure or Breach:

Additional Information:

APPENDIX C – STANDARDS: INFORMATION TECHNOLOGY SERVICES

Standards | Information Technology Services

4-OP-H-25.01 Data Security Standard | Information Technology Services

4-OP-H-25.02 Information Privacy Standard | Information Technology Services

4-OP-H-25.03 IT Security Configuration Management Standard | Information Technology Services

4-OP-H-25.04 IT Network Security Standard | Information Technology Services

4-OP-H-25.05 Bring Your Own Device Standard | Information Technology Services
4-OP-H-25.06 IT Security and Privacy Training Standard | Information Technology Services

4-OP-H-25.07 IT Access, Authorization and Authentication Standard | Information Technology Services

4-OP-H-25.08 IT Physical Security Standard | Information Technology Services

4-OP-H-25.09 IT Vulnerability Management Standard | Information Technology Services

4-OP-H-25.10 IT Log Collection, Analysis and Retention Standard | Information Technology Services

4-OP-H-25.11 IT Incident Response Standard | Information Technology Services

4-OP-H-25.12 IT Disaster Recovery Planning Standard | Information Technology Services

4-OP-H-25.13 IT Third-Party Vendor Management Standard | Information Technology Services

4-OP-H-25.14 Encryption Standard | Information Technology Services

4-OP-H-25.15 IT Data Disposal and Media Sanitization Standard | Information Technology Services

4-OP-H-25.16 IT Application Secure Coding Standard | Information Technology Services

4-OP-H-25.17 IT Enterprise Integration Security Standard | Information Technology Services

4-OP-H-25.18 Risk Management Standard | Information Technology Services

4-OP-H-25.19 Defining Consolidated University Units Standard | Information Technology Services

4-OP-H-25.20 Request for Exception to IT Security Policy | Information Technology Services

APPENDIX D – TECHNOLOGY: POLICIES AND PROCEDURES

4-OP-H-4 Telecommunication Services | Policies and Procedures

4-OP-H-7 University Cellular Communication Services Allowance Policy | Policies and Procedures

4-OP-H-13 Electronic Mail Policy | Policies and Procedures

4-OP-H-14 Mobile Applications, Digital Services, Social Media, and Mobile Messaging | Policies and Procedures

4-OP-H-20 Information Technology Security and Information Assurance Policy | Policies and Procedures

4-OP-H-21 Acceptable Use of Technology Policy | Policies and Procedures

4-OP-H-22 Privacy Policy | Policies and Procedures

4-OP-H-30 Health Insurance Portability and Accountability Act (HIPAA) Policy | Policies and Procedures

4-OP-H-30.01 Designation of University Health Care Components | Policies and Procedures

4-OP-H-30-02-Acknowledgement-of-Understanding-and-Compliance.pdf

4-OP-H-31 HIPAA Authorization for Use and Disclosure of Protected Health Information Policy | Policies and Procedures

4-OP-H-32 Gramm Leach Bliley Act (GLB) Policy | Policies and Procedures