UCF Security Incident Response Plan
UCF Security Incident Response Plan

PREAMBLE: To properly respond in a consistent manner, with appropriate leadership and technical resources, to a security incident that threatens the confidentiality, integrity and availability of information resources or violations of acceptable use policy.

A swift response to a security incident that threatens the confidentiality, integrity, and availability of university information assets and the networks that deliver the information, is required to protect those assets. Without a rapid response, those assets could be compromised, and the University could be in violation of Federal, State, and Local statutes and in violation of its own policies.

The security incident response process may start with an explicit report of a security breach, but it is more likely to start as the result of a routine investigation into some anomalous system or network behavior. For example, a server may be operating slowly, or the printing service may stop working. Because of the potential for unauthorized release or modification of data, in addition to service disruption, it is important to assess the possibility that strange behavior may be the result of some security problem before taking steps to correct a “normal” problem.

When it is determined that an incident may be security related, then the nature of the recovery effort must be modified and appropriate personnel need to be involved to ensure that appropriate information is collected and documented to determine the nature and scope of the security incident and, if appropriate, to facilitate an investigation by law enforcement. Depending on the nature and scope of a breach, it may be necessary to make public disclosure which will require the involvement of campus executives and managers.

SCOPE: This plan applies to all university information systems and services with the exception of disaster recover procedures.

PROCEDURES: The Security Incident Response Flowcharts provide the process for responding to a security-related incident. While following this process, it is important to keep the following in mind:

- Discovery
  - The security incident response process may start with an explicit report of a security breach, or from a routine investigation into some anomalous system or network behavior, or from a vulnerability scan results, or from internal sources reporting of violations of acceptable use policy, or suspicious activities from intrusion prevention systems and similar monitoring tools, or from 3rd party reports.

- Document
  - The key to proper investigation is proper documentation. The discovery of a security incident needs to be properly documented within university's enterprise ITSM tool.

- Notification
  - Information must be shared with individuals involved in the investigation.
  - It is important that all members of the Security Incident Response Team are up to date as events unfold. Much of the information, however, may be confidential, so care should be taken to protect confidentiality of discussions.
• Acknowledgment
  o Initial notifications regarding a security incident must be acknowledged to demonstrate action will be taken immediately to contain the incident

• Containment
  o Swift containment is necessary to prevent the spread of malware, further compromise or disclosure of information. Containment of the incident and investigation may be pursued simultaneously

• Investigation
  o After an incident has been contained, system can be freely investigated. Document all action taken in university's enterprise ITSM tool

• Eradication
  o Eradication may be necessary to eliminate components of the incident such as deleting malicious code or disabling breached user accounts

• Recovery
  o Recover to normal operations
  o Harden systems or processes to prevent similar incidents

• Closure
  o Review incident and close open incidents

Security Incident Response Advisory Committee

Security Incident Response Advisory Committee oversees or directly manages the response to data security incidents and collaborates with data stewards to ensure effective procedures for identifying suspected or actual data breaches. Committee members are from appropriate units deemed necessary to provide expertise and engage in a collaborative way to respond to information security incidents. The following are examples of positions and organizational units who are part of the Security Incident Response Advisory Committee:

<table>
<thead>
<tr>
<th>Positions, Unit</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vice President and CIO, Information Technologies &amp; Resources</td>
<td>Strategic direction and guidance</td>
</tr>
<tr>
<td>CISO, Information Security Office</td>
<td>Strategic direction and guidance</td>
</tr>
<tr>
<td>Associate Vice President and COO, UCF IT</td>
<td>Strategic direction and guidance</td>
</tr>
<tr>
<td>Director of Compliance and Ethics, Office of Compliance &amp; Ethics</td>
<td>Compliance expertise and support</td>
</tr>
<tr>
<td>Chief Audit Executive, University Audit</td>
<td>Investigative expertise and support</td>
</tr>
<tr>
<td>Deputy General Counsel, Office of the General Counsel (OGC)</td>
<td>Regulation and policy expertise and support</td>
</tr>
<tr>
<td>Assistant Vice President, Communication &amp; Marketing</td>
<td>Public communications and responding to the press</td>
</tr>
<tr>
<td>UCF Police</td>
<td>Law enforcement expertise</td>
</tr>
<tr>
<td>Other divisions, departments or units when necessary.</td>
<td>Local expertise within their own IT environment</td>
</tr>
</tbody>
</table>
Security Incident Response Team (SIRT)

Responsibilities of the SIRT are investigation and reporting. In order to carry out these responsibilities, the following support activities will be performed by the SIRT:

- SIRT continually updates the Security Incident Response Plan
- SIRT maintains systems for discovering security incidents
- SIRT documents IT security incidents in a tracking system
- SIRT will coordinate IT security incidents from discovery to closure
  - SIRT reviews incidents, provides solutions/resolutions and closure.
- SIRT will assess threats to IT resources
- SIRT will process IT security complaints or incidents
- SIRT will alert IT managers of imminent threats
- SIRT determines incident severity and escalates it, if necessary, with notification to Security Incident Response Advisory Committee.
Incident severity classification

Unrestricted Data

- Data not protected by law or contract, or whose disclosure would cause no harm to the university or to individuals
- Local SysAdmin responsible for containment, investigation, rebuild, and hardening system. Properly document the incident, report to Department Security Liaisons, SysAdmins, SIRT, closure.

Restricted Data

- Data whose unauthorized access, modification or loss could adversely affect the university (e.g., cause financial loss or loss of confidence or public standing in the community), adversely affect a partner (e.g., a business or agency working with the university), or adversely affect the public.
  - Examples, business sensitive information, system or network information, network and system IDs, student grades, etc.
- Disclosure of such data should pose no harm (financial or physical) to an individual.
- Local Admin and SIRT are responsible for the response based on SIRT Plan.
- Breach of Restricted Data will generally not require notification or an announcement.

Highly Restricted Data

- Data including Personally Identifiable Information (PII): a) information from which an individual may be uniquely and reliably identified or contacted, including an individual’s social security number, account number, and passwords; b) information protected under the FERPA regulations and other “non-directory” information interpreted by the University; c) information concerning an individual that is considered “nonpublic personal information” within the meaning of Title V of the Gram –Leach Bliley Act of 1999 (Public Law 106-102, 11 Stat. 1338) (as amended) and its implementing regulations, and; d) information concerning an individual that is considered ”protected health information” within the meaning of the Health Insurance Portability and Accountability Act of 1996 (as amended), and its implementing regulations. Protection for such data may also be subject to additional operating regulations in accordance with vendor or partner agreements, such as the Payment Card Industry Data Security Standards (PCI DSS)
- Local Admin and SIRT are responsible for the response based on SIRT Plan.
- Breach of Highly Restricted Data will generally require notification to affected individuals and/or a public announcement.
General Incident Response Process

Process

Pre-Incident

Incident Detection

Notification to Systems administrator and ISO

System administrator conducts initial investigation and document findings

Is it really an Incident?

No

Yes

Activate SIRT

SIRT investigates and determines initial response

Is it really an Incident?

No

Yes

People

Third party, internally reported, SIRT, SOC, NetSec

SIRT, SOC or NetSec

SysAdmin, SIRT member or delegate

SIRT

CIO, CISO, COO, VP

SIRT

SIRT
Execute Response strategy based on this plan

Communicate as appropriate

Continue Investigation and Restoration and document findings

Collect Evidence

Preserve log files

Forensic backup if necessary

Monitor system and network

Return to normal operation

Identify and implement security/lessons learned

Closure

- - - - -

SIRT

- - - - -

SIRT notifies Department Security Liaisons, Dean, Chair, VP, GCO, UCF News & Info

- - - - -

SysAdmin, SIRT

- - - - -

SysAdmin, NetSec, UCF Technology Based Crime Unit (TBCU), IRR

- - - - -

SysAdmin

- - - - -

SysAdmin, SIRT, SOC, NetSec

- - - - -

SIRT