UCF Security Incident Response Plan

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476

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 pan 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 suspicions 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

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476

- Acknowledgment
  - Initial notifications regarding a security incident must be acknowledged to demonstrate action will be taken immediately to contain the incident
- Containment
  - 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
  - After an incident has been contained, system can be freely investigated. Document all action taken in **university's enterprise ITSM tool**
- Eradication
  - Eradication may be necessary to eliminate components of the incident such as deleting malicious code or disabling breached user accounts
- Recovery
  - Recover to normal operations
  - Harden systems or processes to prevent similar incidents
- Closure
  - 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 collaborate 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:

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

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution

Information Security Office
Security Incident Response Team
SIRT@ucf.edu

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.

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution

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

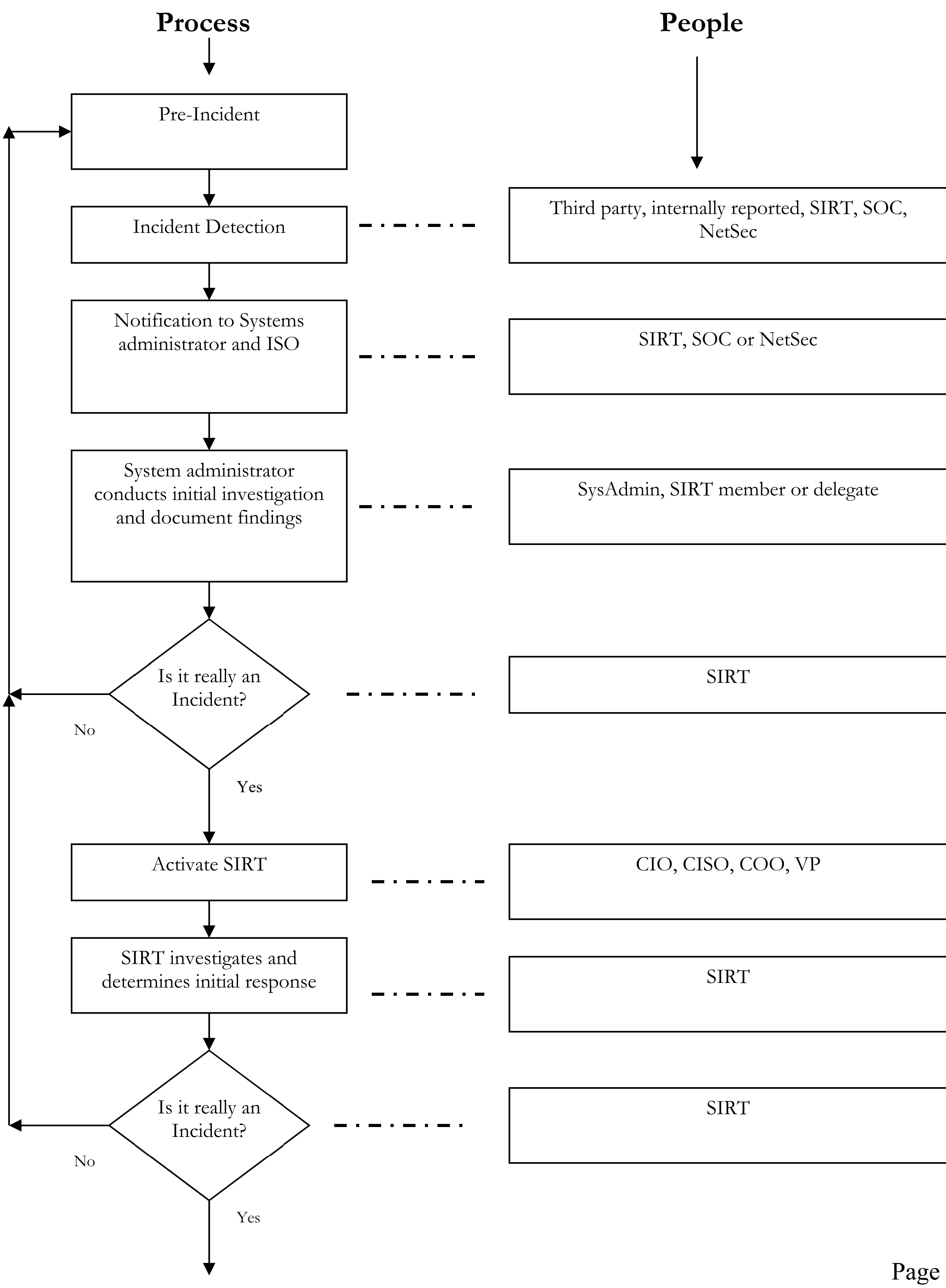
- *Data whose unauthorized access, modification or loss could adversely affect the university (e.g., cause financial loss or loss of confidence or public standing in the community), adversely affect a partner (e.g., a business or agency working with the university), or adversely affect the public.*
    - *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

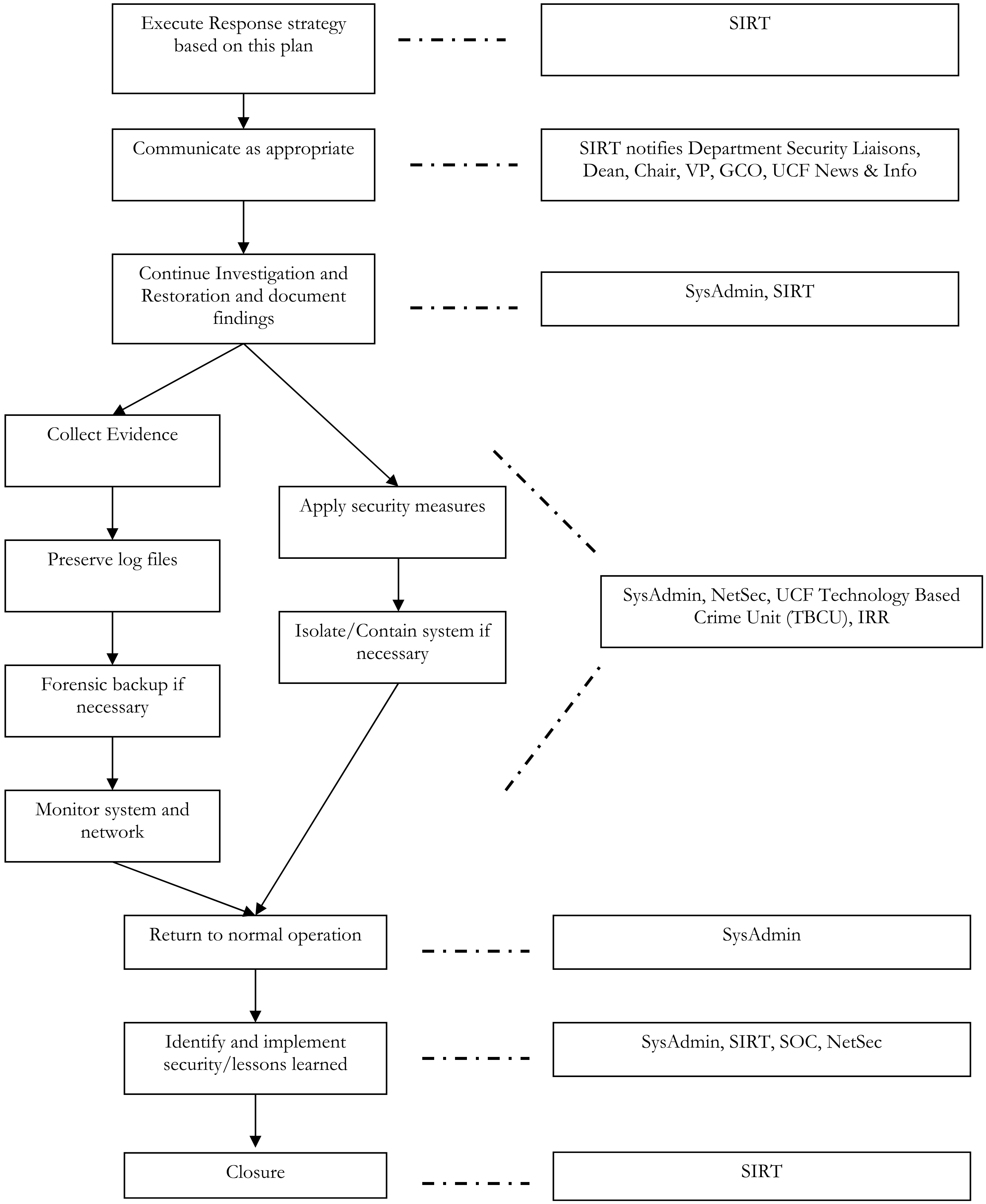
- *Data including Personally Identifiable Information (PII): a) information from which an individual may be uniquely and reliably identified or contacted, including an individual's social security number, account number, and passwords; b) information protected under the FERPA regulations and other "non-directory" 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.**

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476

General Incident Response Process



Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476



Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution