UCF Security Incident Response Plan

High Level

Chris Vakhordjian
Information Security Officer
Computer Services & Telecommunications
Division of IT&R
Revision 1.1, 7 June 2007

UCF Security Incident Response Plan

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

A swift response to an 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, or 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 breach 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 procedure 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 a formal infringement notification from the RIAA or DMCA, or from internal sources reporting of violations of acceptable use policy, or suspicions activities from intrusion detections systems, etc.
- Document
    - The key to proper investigation is proper documentation. The discovery of an incident needs to be properly documented within the NOC incident response web site
- 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
  - Initial notifications regarding an 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 worms, 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 the NOC incident response web site
- 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

The CS&T Security Incident Response Team (SIRT)

The UCF Information Security Officer will select CS&T staff from selected CS&T Organizational Units deemed technically proficient to provide assistance in his/her specific area to work collaboratively in responding to a security incident. The following CS&T Organizational units will be used for SIRT:

Unit	Purpose
UCF Information Security Office	ISO's direction and supervision
ITR	CIO's direction and supervision
CTO	CTO's direction and supervision
NOC Security Group	Networking security expertise
NOC/TeleData	Network and Helpdesk expertise
Computer Shop	System and hardware expertise
UCF Technology Based Crime Unit	Forensic expertise
CS&T Systems Group	Systems expertise
Technology Integrators Group	Programming expertise
Local SysAdmin, head IT, IT manager, etc., or other units when necessary	Local expertise within their own IT environment
General Counsel's Office (GCO)	Regulation and policy expertise
UCF News and Information	Public communications and responding to the press

The UCF Information Security Officer may from time to time add additional staff or deputize departmental ITes for the process of investigating a security incident.

The Security Incident Response Team (SIRT) is tasked with the following responsibilities:

- SIRT continually updates the Security Incident Response Plan

- SIRT maintains systems for discovering security incidents involving UCF IT resources
- SIRT documents IT security incidents in a tracking system (*soon to be within Remedy*)
- SIRT will coordinate IT security incidents (level 2/3) from documentation 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 CIO, CTO, and ISO.

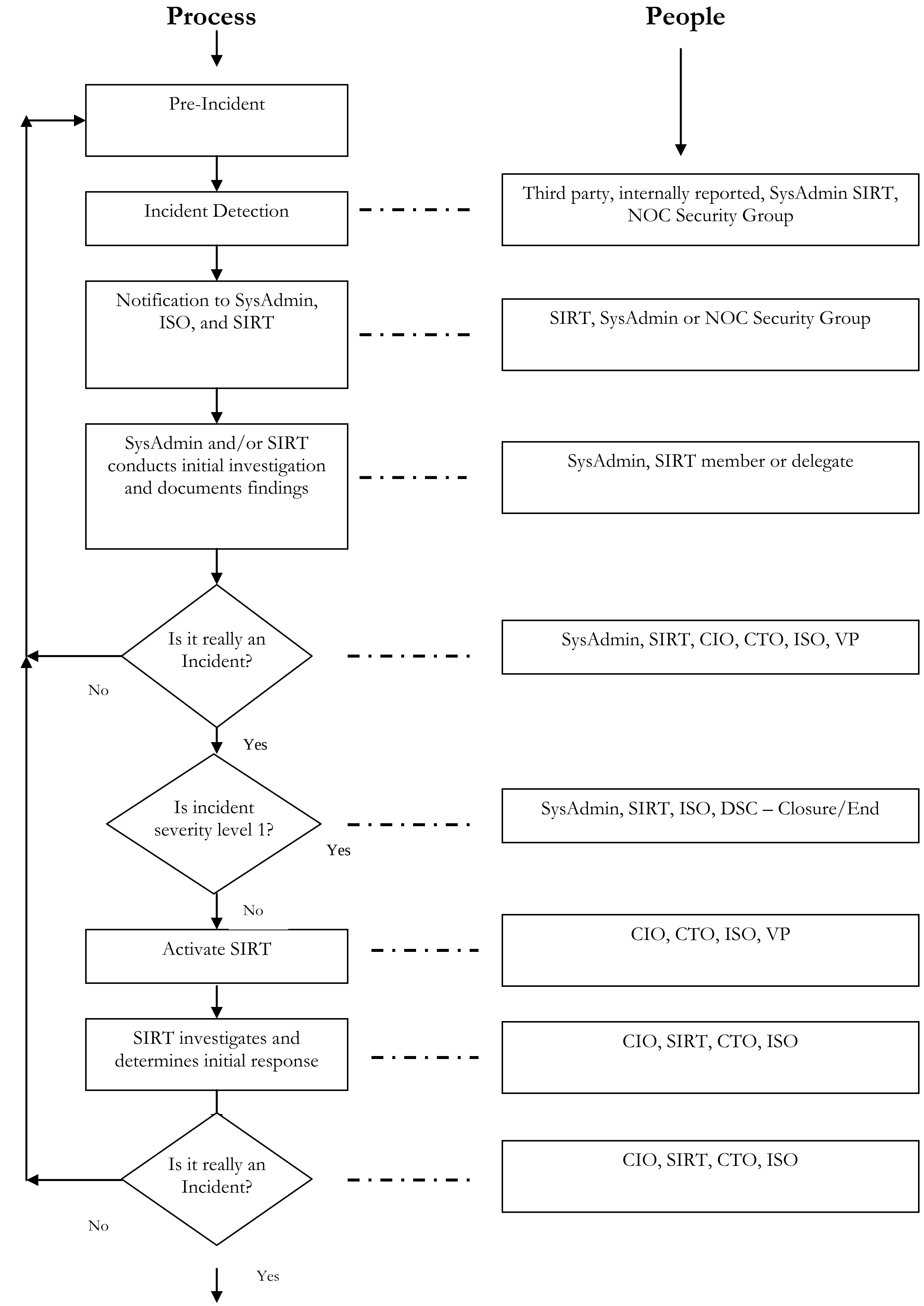
Incident severity classification

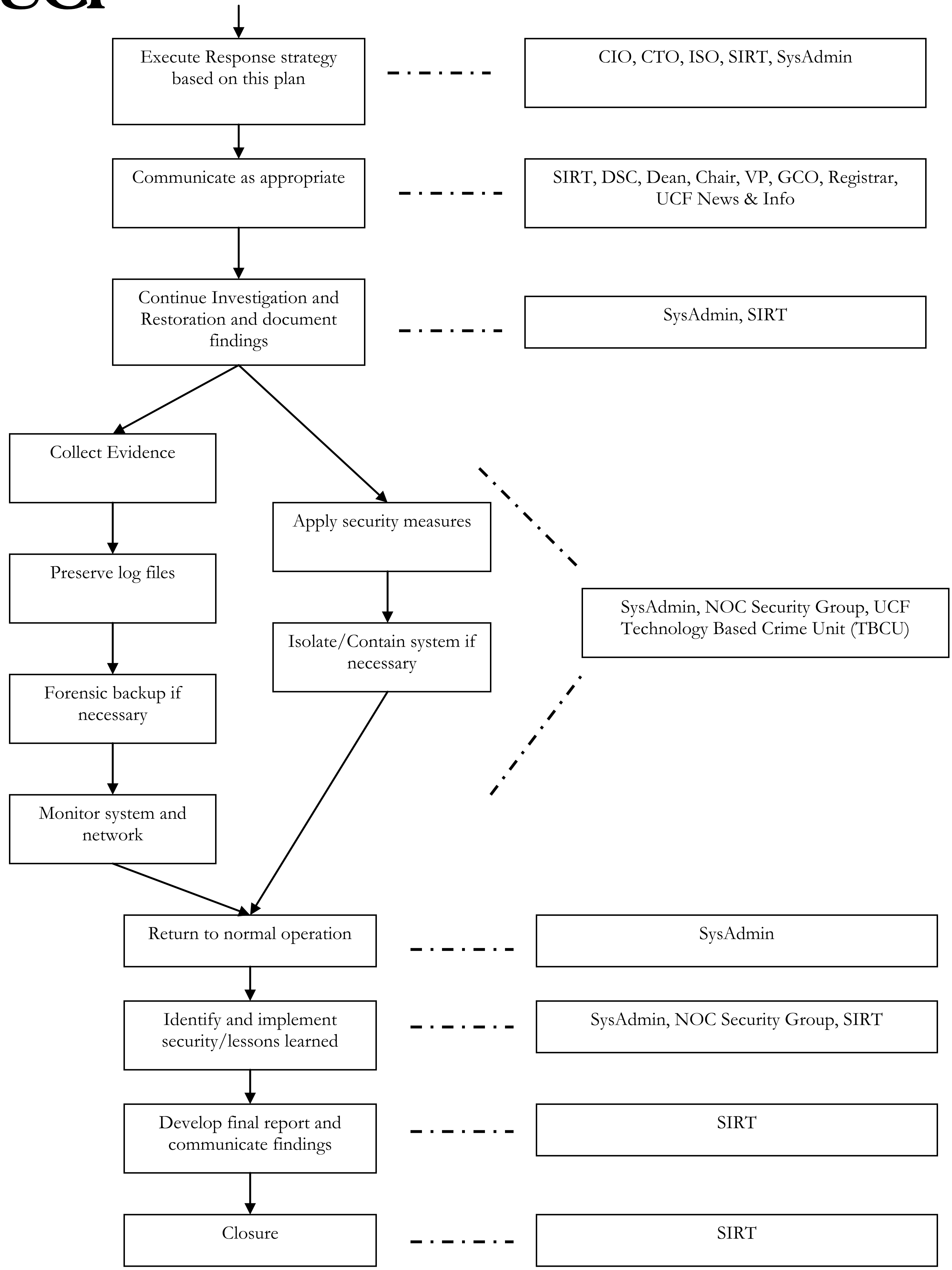
- Level 1 Incident – Security incident involving Unrestricted Data
    - *Data not protected by law or contract, or whose disclosure would cause no harm to the university or to individuals*
    - **Local SysAdmin responsible for containment, investigation, rebuild, and hardening system. Properly document the incident, report to DSC, SysAdmins, SIRT, closure.**
    - **Contact SIRT at sirt@mail.ucf.edu with details of the compromise**

- Level 2 Incident – Security incident involving Restricted (non-personal) 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.*
    - **Local Admin and SIRT (sirt@mail.ucf.edu) are responsible for the response based on SIRT Plan.**

- Level 3 Incident – Security incident involving Restricted (personal) 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 (sirt@mail.ucf.edu) are responsible for the response based on SIRT Plan.**

General Incident Response Process


Process
People
Pre-Incident
Incident Detection
Third party, internally reported, SysAdmin SIRT, NOC Security Group
Notification to SysAdmin, ISO, and SIRT
SIRT, SysAdmin or NOC Security Group
SysAdmin and/or SIRT conducts initial investigation and documents findings
SysAdmin, SIRT member or delegate
Is it really an Incident?
SysAdmin, SIRT, CIO, CTO, ISO, VP
No
Yes
Is incident severity level 1?
SysAdmin, SIRT, ISO, DSC – Closure/End
Yes
No
Activate SIRT
CIO, CTO, ISO, VP
SIRT investigates and determines initial response
CIO, SIRT, CTO, ISO
Is it really an Incident?
CIO, SIRT, CTO, ISO
No
Yes


Execute Response strategy based on this plan
CIO, CTO, ISO, SIRT, SysAdmin
Communicate as appropriate
SIRT, DSC, Dean, Chair, VP, GCO, Registrar, UCF News & Info
Continue Investigation and Restoration and document findings
SysAdmin, SIRT
Collect Evidence
Apply security measures
Preserve log files
Isolate/Contain system if necessary
SysAdmin, NOC Security Group, UCF Technology Based Crime Unit (TBCU)
Forensic backup if necessary
Monitor system and network
Return to normal operation
SysAdmin
Identify and implement security/lessons learned
SysAdmin, NOC Security Group, SIRT
Develop final report and communicate findings
SIRT
Closure
SIRT