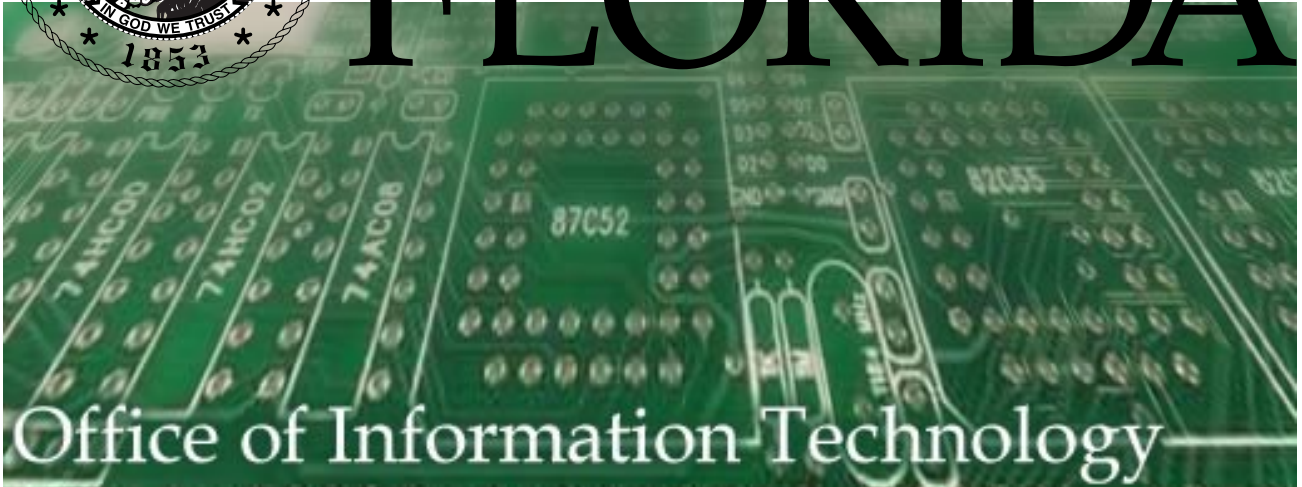


UNIVERSITY OF  
FLORIDA



Office of Information Technology

# UF Information Technology Security Regulations

*March 15, 2005*

This page intentionally left blank

# Contents

<b>UF Information Technology Security Charter .....</b>	<b>5</b>
<b>Introduction .....</b>	<b>5</b>
<b>Mission and Objectives .....</b>	<b>5</b>
<b>Scope .....</b>	<b>5</b>
<b>Enforcement .....</b>	<b>6</b>
<b>Definitions .....</b>	<b>6</b>
<b>Roles and Responsibilities .....</b>	<b>7</b>
<b>UF IT Resource Categories .....</b>	<b>10</b>
<b>UF Information Technology Security Policies .....</b>	<b>11</b>
<b>General Rules .....</b>	<b>11</b>
<b>Policies .....</b>	<b>12</b>
<b>Standards and Procedures .....</b>	<b>13</b>
<b>UF Network and Host Security Standard .....</b>	<b>13</b>
<b>Authentication and Authorization Standard .....</b>	<b>13</b>
<b>Network Security Standard .....</b>	<b>13</b>
<b>Node Security Standard .....</b>	<b>14</b>
<b>Standard for Hosts Managed by Associates .....</b>	<b>15</b>
<b>Procedures for Hosts Managed by Associates .....</b>	<b>15</b>
<b>Software Security Standard .....</b>	<b>16</b>
<b>Change Management Standard .....</b>	<b>17</b>
<b>UF IT Security Incident Response Standard .....</b>	<b>18</b>
<b>Critical IT Resources Standard .....</b>	<b>18</b>
<b>Procedures to Register Critical IT Resources .....</b>	<b>19</b>
<b>Service Interruption Notification Procedures .....</b>	<b>19</b>
<b>Incident Response Procedures for Vulnerabilities .....</b>	<b>19</b>
<b>Incident Response Procedures for Compromised IT Resources .....</b>	<b>20</b>
<b>Incident Response Procedures for Copyright Infringement .....</b>	<b>23</b>
<b>Response Procedures for Incidents Involving Law Enforcement .....</b>	<b>25</b>
<b>Incident Response for Non-criminal, Legal Issues .....</b>	<b>25</b>
<b>Incident Response Procedures for Violations of the UF Acceptable Use of             Computing Resources policy (AUP) .....</b>	<b>25</b>

**UF IT Security Physical Security Standard .....27**  
    **UF Physical Security Procedures ..... 27**  
**UF IT Security Risk Assessment Standard ..... 29**  
    **UF Risk Assessment Procedures..... 29**  
**UF IT Security Training and Awareness Standard ..... 31**  
    **Training and Security Awareness Procedures ..... 31**  
**UF IT Security Continuance of Operations Standards ..... 33**  
    **Continuance of Operations Guidelines ..... 33**

# UF Information Technology Security Charter

## Introduction

This charter defines the mission and objectives of the University of Florida (UF) Information Technology (IT) security program, outlines the scope of the organization's mandate, defines terms, and delineates roles and responsibilities for information security throughout the organization. Enforcement rules are also included in this charter.

Unauthorized access, breach of confidentiality, loss of integrity, disruption of availability, and other risks threaten UF IT resources. UF IT security policies are aimed at reducing exposure to threats, thereby minimizing risk in order to protect UF IT resources. Policies are goals or mandates used to cultivate standards. UF IT security standards define metrics against which results can be measured to determine compliance with the policies and describe objectives for procedures. UF IT security procedures detail how to implement standards in order to comply with policies.

## Mission and Objectives

As part of its educational mission and strategic plan to provide state-of-the-art information technology to meet the needs of faculty and students in research and teaching, the University of Florida (UF) acquires, develops, and maintains data and information, computers, computer systems and networks. These information technology (IT) resources are intended for university related purposes, including direct and indirect support of the university's instruction, research and service missions; university administrative functions; student and campus life activities; and the free exchange of ideas within the university community and among the university community and the wider local, national, and world communities.

The mission of the UF information security program is to support the goals of UF by assuring the availability, integrity and appropriate confidentiality of information. Primary objectives include development and implementation of proactive measures to prevent security problems and effective response to security problems when prevention methods are defeated.

## Scope

This charter applies to all people who maintain or manage university IT resources, their supervisors and their unit administrators. It applies to all locations of those resources, whether on campus or remote locations. It applies to all UF and unit policies, standards and procedures, some of which are listed below. This charter is intended to help protect integrity, availability, accountability and appropriate confidentiality of UF IT resources. Additional standards and procedures may govern specific data, computers, computer systems or networks provided or operated by specific UF and subsidiary units.

# UF Information Technology Security Regulations

Acceptable Use of Computing Resources  
UF Policy for Security Management Responsibilities  
UF Physical Security Standard  
UF Network Security Standard  
UF Software Security Standard  
UF Risk Assessment Standard  
UF Incident Response Standard  
UF IT Training and Security Awareness Standard  
UF Data Security Standard  
Business Resumption Standard

## Enforcement

Unit administrators and IT workers who fail to adhere to this charter may be subject to penalties and disciplinary action, both within and outside the university. Violations will be handled through the university disciplinary procedures applicable to the relevant Unit or IT employee. The university may temporarily suspend, block or restrict access to IT resources, IT workers, and/or Units independent of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of university or other IT resources or to protect the university from liability. The university may also refer suspected violations of applicable law to appropriate law enforcement agencies.

## Definitions

### **UF Unit:**

College, Department, Research Center, Institute or other administrative subdivision connected to the University of Florida network.

### **Subsidiary Unit:**

A major unit which has a distinct and divergent mission statement from that of UF, and which in some cases may also be a separate legal entity, such as Shands.

### **Associate:**

An entity external to UF that performs functions or activities that involve the use or disclosure of information on behalf of, or provides services to, the University.

### **IT resource:**

Any equipment used to store, process, display or transport digital information is an IT resource. The associated data, applications and hardware, are also IT resources.

### **Information Technology (IT) worker:**

An individual hired by a unit to manage or maintain IT resources in that unit. IT duties must be specified in the job description.

# Roles and Responsibilities

UF information security roles are organized in three main levels: Level 1 has responsibility for the entire university, Level 2 units are listed below, and Level 3 has responsibility for smaller units within Level 2 units. More levels may be added at the discretion of those responsible for Level 2.

Level 1 roles are UF Information Security Administrator (ISA) and UF Information Security Manager (ISM). Level 2 roles are Unit ISA and Unit ISM. The organizational structure for Level 3 and lower security contacts is defined by the Level 2 Unit ISA and Unit ISM. Level 3 and lower security contacts must work within the organizational structure established by their unit. To avoid confusion with Level 2 security titles, units must specify the level as part of Level 3 and lower titles, such as 'Level 3 Unit ISA' or 'Level 3 Unit ISM'.

## **Level 2 units are:**

- Office of Finance and Administration
- Bridges
- Office of the Provost and Senior Vice President
- Division of Student Affairs
- Department of Housing and Residence Education
- Office of the University Registrar
- Research and Graduate Programs
- Libraries
- Computing and Networking Services
- Office of Academic Technology
- College of Business
- College of Design, Construction, and Planning
- College of Education
- College of Engineering
- College of Fine Arts
- College of Health and Human Performance
- College of Journalism
- College of Law
- College of Liberal Arts and Sciences
- Institute of Food and Agricultural Sciences
- Health Science Center
- Interdisciplinary Center for Biotechnology Research
- National Center for Construction Education and Research
- International Center
- Latin American Studies
- P. K. Yonge Developmental Research School
- Florida Museum of Natural History
- Division of Continuing Education
- University of Florida Foundation
- Florida Center for Library Automation
- Shands HealthCare
- University Athletic Association
- University Press of Florida

# UF Information Technology Security Regulations

Division of Plant Industry  
United States Department of Agriculture  
Oak Hall School  
Alachua Freenet  
Cox Cable

## **UF IT Security Administrator (UF ISA)**

The UF ISA has the responsibility to ensure implementation and management of the UF IT security program. The UF ISA has the authority to direct action as needed to protect UF IT resources. The UF ISA has the authority to enforce UF IT policies, standards, and procedures and to direct action related to violations. Where questions arise with respect to what constitutes a unit, the UF ISA has final authority.

## **UF IT Security Manager (UF ISM)**

The UF ISM manages the UF IT security program and security team. The UF ISM is responsible for coordinating efforts to create and maintain centralized UF IT security policies, standards, and procedures. The UF ISM or a designee is responsible for enterprise risk assessment, enterprise network intrusion detection, working with Level 2 Unit ISMs to resolve exposures and reduce potential exposures, the UF security web site, and organizing IT security training and awareness events. The UF ISM is responsible for maintaining only Level 2 Unit ISA and Unit ISM contact information. Level 2 Unit ISAs and ISMs are listed in the contact database maintained by Network Services.

IT duties must be specified in the job description of the UF ISM.

## **Level 2 Unit IT Security Administrator (Unit ISA)**

At a minimum, security authority and responsibility must be defined at the division or college level. The highest level unit administrator is the Level 2 Unit ISA, but this authority may be delegated. IT security responsibilities and reporting structure within the unit are at the discretion of the Level 2 Unit ISA, but a structure based to the UF structure is recommended with security administrators and security managers designated in each sub-unit.

The Level 2 Unit ISA has the responsibility to ensure implementation and management of the units IT security program. They have the authority to direct action as needed to protect unit IT resources. They have the authority to enforce UF and unit IT policies, standards, and procedures and to direct action related to violations. Each Level 2 Unit ISA must appoint an Level 2 Unit Information Security Manager (Unit ISM). The higher level unit has the discretion to designate ISMs at subordinate unit levels, but contact information must be maintained by the Level 2 Unit ISM.

Where appropriate, IT duties must be specified in the job description of the Level 2 Unit ISA.

## **Level 2 Unit IT Security Managers (Unit ISM)**

Level 2 Unit ISMs are responsible for managing and coordinating security efforts within that unit's organizational hierarchy. The Level 2 Unit ISM has the responsibility to advise unit administration of security implementations consistent with UF IT policies, standards, and procedures. While the Level 2 Unit ISM is responsible to their unit administrative structure, they must be made known to the UF ISM.

## UF Information Technology Security Regulations

To ensure professional management of UF IT resources, the Level 2 Unit ISM must ensure that their unit complies with UF IT security policies, standards, and procedures and that employees in their unit are aware of applicable laws, policies, standards, and procedures.

All units must have specific written IT security policies, standards and procedures. The Level 2 Unit ISM, in cooperation with the Level 2 Unit ISA, is responsible for the coordination of unit IT security policies, standards, and procedures. Unit security policies, standards, and procedures must be available to the UF ISM upon request. Units must create standards for physical access, network and host access, incident response, data security, business resumption, awareness, etc.

It is possible that ISM duties for smaller units do not require a full-time commitment and may be assigned to an existing IT position. IT duties must be specified in the job description of the Level 2 Unit ISM. The Level 2 Unit ISM must coordinate with their unit administration to ensure that all networks in their unit have adequate professional coverage, including vacation alternates. The Level 2 Unit ISM must maintain contact information for their unit IT staff and appropriate alternates. The Level 2 Unit ISM must ensure that all people who manage IT resources in their unit are appropriately trained and aware of relevant laws, and UF policies, standards, and procedures. The Level 2 Unit ISM must coordinate within their unit various IT security responsibilities, including but not limited to monitoring, documenting, reporting, and correcting the cause of security breaches, establishing minimum security standards for the installation and configuration of IT resources, maintaining the operating systems, reviewing account termination, ensuring secure coding, and other security functions.

The Level 2 Unit ISM must be a permanent employee with more than 50% IT related job responsibility. They must have a high school diploma or equivalent, and at least 4 years of professional IT related job experience. IT related vocational training or college course work may substitute for experience. The Level 2 Unit ISM must be a full-time employee. An FBI background check is recommended for all people who maintain or manage IT resources, but is required before an individual is assigned Level 2 Unit ISM duties. Existing employees not on probation at the time this charter is implemented do not require an FBI background check.

The Level 2 Unit ISM should pursue IT security related continuing education such as Information Technology Security Awareness Day.

### **IT workers**

IT workers maintain, manage, or have responsibility for UF IT resources. All IT workers must be qualified to implement UF and respective unit IT policies, standards, and procedures appropriate to their level of job responsibility, or they must be closely supervised by someone who is. Where questions arise with respect to qualifications of IT worker candidates, the hiring authority must coordinate with the Level 2 Unit ISM and the Unit ISA

IT duties must be included in job descriptions of IT workers.

IT workers are responsible to keep informed of changes to UF and respective unit IT policies, standards, procedures, and other information resources.

# UF IT Resource Categories

In terms of management and responsibility, the University of Florida recognizes the following categories of IT resources: professionally managed, personally managed, and managed by business associates. These categories are described below.

## **Professionally Managed IT Resources**

Professionally managed IT resources are maintained by IT workers in a manner consistent with UF IT policies, standards, and procedures. Non-IT workers should not manage UF IT resources. Qualified professional IT consultants may be contracted to manage or maintain unit IT resources, but must comply with UF and respective unit IT policies, standards, and procedures. If the unit cannot support IT workers, they should seek assistance from IT workers in another unit or contact the UF ISM.

## **Personally Managed IT Resources**

All UF IT resources must be managed by UF IT workers. The Level 2 Unit ISA can make exceptions for research or other purposes and allow non-IT workers to manage IT resources. These are referred to as personally managed IT resources. Personally managed IT resources also include personally owned devices such as laptops, computers, PDAs, and other IT equipment. Personally managed IT resources commonly connect in classrooms, at walkups, with wireless, and on the student residential network. Personally managed IT resources must meet the following requirements.

Before connecting to the UF Network, personally managed IT resources must connect only to designated network zones.

All personally managed IT resources connecting to unit networks must be coordinated with the Level 2 Unit ISM

The Level 2 Unit ISM must ensure that maintainers of personally managed IT equipment in their unit are aware of relevant UF IT security policies, standards, and procedures.

The Level 2 Unit ISM must ensure that maintainers of personally managed IT resources comply with relevant UF IT security policies, standards, and procedures.

## **IT Resources Managed by Associates**

Associates that manage IT resources on the UF network must be informed of UF IT security policies and sign an agreement to comply with them. UF and Level 2 Unit ISMs must maintain contact information for all Associates managing IT resources on networks for which they are responsible. Requests for exceptions to this policy must be submitted in writing by the Level 2 Unit ISM to Information Technology Advisory Committee - Information Security Management (ITAC-ISM). The UF ISM will respond to all requests for exceptions in writing. For procedures related to hosts managed by business associates, see the Network and Host Security Standard.

# UF Information Technology Security Policies

## General Rules

All UF IT security measures must comply with federal and state laws, university rules and policies, and the terms of applicable contracts including software licenses. Examples of applicable laws, rules and policies include the laws of libel, privacy, copyright, trademark, obscenity and child pornography; the Florida Computer Crimes Act, the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking," "cracking" and similar activities; the university's Student Code of Conduct; the university's Sexual Harassment Policy. IT workers with questions as to how the various laws, rules and resolutions may apply to a particular use of university computing resources should contact the Office of the General Counsel or their appropriate legal services for more information.

Security has the potential to impact usability. Where usability and security seem to be in conflict, IT workers must coordinate with their Level 2 Unit ISA and Unit ISM to implement a solution that enables all users to reliably perform their essential University job functions in the most secure manner consistent with applicable laws, policies, standards, and procedures. Units are expected to provide careful oversight to ensure that a balance between security and productivity is maintained. Ideally, responsibility for security management and for day-to-day operation are assigned to different individuals of equal authority. Security managers should not be subordinate to managers of day-to-day operation.

Requests for exceptions to this charter must be submitted in writing by the Level 2 Unit ISM to the Information Technology Advisory Committee on Information Security Management (ITAC-ISM) for review. The UF ISM will respond to all requests for exceptions in writing.

These policies will be reviewed and updated by ITAC-ISM as needed, but at a minimum every three years.

# Policies

1. The confidentiality, integrity and availability of UF IT resources must be ensured. However, availability of IT resources may be temporarily suspended, blocked or restricted when it is reasonably necessary to protect UF IT resources or liability.
2. All IT workers must be aware of the duties and responsibilities of their position with respect to IT security, and comply with all applicable laws, policies, standards, and procedures.
3. An auditing system must be in place to identify use of UF IT resources.
4. UF IT resources must be protected from unauthorized access.
5. All IT resources must be made as robust against unauthorized use or attack as possible, consistent with providing necessary services.
6. The security implications of all changes to IT resources must be considered.
7. Security incidents impacting confidentiality, integrity or availability of IT resources must be investigated, documented, reported and resolved in a timely manner.
8. A plan must be documented for the recovery from incidents impacting confidentiality, integrity, or availability of IT resources.

# Standards and Procedures

## UF Network and Host Security Standard

### Authentication and Authorization Standard

Access to UF IT resources must be restricted to authorized methods. Facilities must be established to identify who was using any node on the network and when they were doing so. Access methods must be sanctioned by the Level 2 Unit ISM. Access must be logged and each log entry must include user identification, network address, hardware address, and an accurate time stamp. Logs must be regularly reviewed for anomalies including unauthorized access. Access logs must be retained for at least three years unless required by law to be retained longer.

Units must establish and document criteria for issuing and revoking accounts used for access. Each UF and subsidiary unit must establish policy and procedures regarding guest access. The unit policy must describe minimum authentication requirements, including password restrictions where applicable.

### Network Security Standard

Nodes, services and individuals shall not have network exposure and visibility beyond that which is necessary for their intended functions. Similar IT resources should be logically aggregated to facilitate network security zone management. In cases where network firewalls are used, they must be documented and coordinated with Network Services.

UF and applicable subsidiary Level 2 Unit ISMs will coordinate and document the establishment of all external network connections for their unit with Network Services. As every external network connection is potentially an entry point for intruders, Level 2 Unit ISMs must document all external network connections in their unit, including modems.

Only network access locations designated by the UF and Level 2 Unit ISM may be used by personally managed IT resources. UF and Level 2 Unit ISMs are responsible for all network access locations used by personally managed IT resources, but are not responsible for the resources themselves. UF and Level 2 Unit ISMs have the responsibility to identify a user connected to a given port at any given time. UF and Level 2 Unit ISMs must be able to instigate disruption of service to the user and/or address. UF and Level 2 Unit ISMs also have the responsibility to coordinate notification to the user and ensure that the incident is resolved. For units that do not provide their own network service, their service provider must provide the functionality described above.

Network access for personally managed IT resources should be more restricted than network access for professionally managed IT resources. Possible restrictions include:

- WIPA authentication where possible.
- A VLAN separate from the professionally managed machines.

- Restriction to private IP only.
- Incoming and outgoing network firewalls or access control lists to prevent commonly exploited network services.
- Restrictions that prevent external hosts from initiating connections.

## Node Security Standard

Before connecting to the UF network, devices managed by UF IT workers must:

1. Have a clearly defined UF purpose and intended user base.
2. Be protected during the installation process by some combination of restricted network access, specific ACLs, private IP, or off-line installation (Best Practices for Secure Installation).
3. Be operated and secured appropriately for its specified network zone.
4. Have appropriate access restrictions, including but not limited to physical, ACL, firewall, authentication, authorization restrictions, screen locks, and inactivity timeouts. Network restrictions must allow access to the UF security scanner.
5. Be on private IP, unless public IP is required.\*
6. Be at current patch levels.\*
7. Have current anti-malware protection.\*
8. Have a specific individual designated as manager.
9. Be documented for recreating the system.\*
10. Be documented for operating the system and troubleshooting.\*
11. Have alerting and/or logging for security-related events or patterns where appropriate.
12. Be reviewed for security-related events or patterns with a frequency appropriate to the system.
13. Run only the services necessary to support its function.
14. Run only software necessary to support its function.\*
15. Be monitored for proper system operation where appropriate.\*
16. Provide system facilities to allow users to secure their data.\*
17. Have been scanned for vulnerabilities within the last 3 months.
18. Comply with appropriate Software Security Standard(s).
19. Comply with appropriate Data Security Standard(s).
20. Have defined power and backup power requirements where appropriate.\*
21. Have defined heat generation data where appropriate.\*
22. Not have trust relationships beyond those required for proper function. Where needed, trust relationships should be based on secure cryptographic methods (e.g., SSH public keys or SSL certificates), and not on IP numbers or domain names alone.\*

23. Be synchronized with an accurate time server.\*

\* This standard recognizes that there is more than one way to secure a device. Alternative methods to secure a device may be used where it is not possible to implement this standard or it interferes with proper device function.

In addition, production servers must:

1. Be located in physically secure space approved by the Level 2 Unit ISM and ISA for production servers.
2. Be routinely backed up, use off-site backup storage, and document restoration testing as appropriate.

### **Standard for Hosts Managed by Associates**

Associates that manage hosts on the UF network must be informed of, and sign an agreement to comply with, appropriate UF policies, standards, and procedures. The Level 2 Unit ISM must maintain contact information for all business associates managing hosts in their unit. Requests for exceptions must be submitted in writing by the Level 2 Unit ISM to ITAC-ISM. ITAC-ISM will make a recommendation regarding the request to the UF ISA. The UF ISA will respond to all requests for exceptions in writing.

### **Procedures for Hosts Managed by Associates**

Associates that maintain hosts connected to the UF network are encouraged to use private IP and should access their host through a UF managed secure tunnel provided by Network Services or the unit. Network Services can restrict access to hosts managed by business associates, but access controls should also be applied on such hosts and the local network. Secure encrypted authentication and communication such as SSH or SSL is encouraged. If passwords are transmitted from business associates to resources on the UF network using clear text protocols, those passwords must be single-use passwords.

## Software Security Standard

It is the responsibility of the Level 2 Unit ISA to ensure that all software provided by the unit is properly licensed. Level 2 Unit ISMs must ensure that users in their units are properly informed of their responsibilities regarding legal use of software. The Level 2 Unit ISM has the responsibility to request the removal of software that does not comply with licensing agreements or copyright law, but it is the responsibility of the user to comply with licensing agreements and copyright law as defined in the UF Acceptable Use Policy. UF IT workers must be aware of and comply with applicable laws and policies regarding their use of software on IT resources they manage.

All software systems must be as robust against unauthorized use or attack as is possible consistent with providing necessary services.

A means for scanning every IT resource for invasive or malicious software must be provided.

The Level 2 Unit ISA has the authority and responsibility to ensure an appropriate level of security of computer applications developed at or intended for use at the University of Florida for processing financial data, student data, health data, mission critical data, intellectual property or any other data that is Sensitive and Critical. This applies to the development process as well as to the deployment process. It is particularly critical for network applications.

Unless the Level 2 Unit ISA has instituted alternative guidelines, it is incumbent upon the developer to demonstrate to the Level 2 Unit ISM that they follow secure application development procedures described in UF Procedures to Develop Applications for Secure Deployment. Security must be considered throughout the coding life cycle including design, implementation, testing, auditing and improvement. A secure application:

1. Is auditable, both in source code and in actual use.
2. Has its design and implementation reviewed by experienced practitioners.
3. Does not rely on just one layer of security.
4. Has been tested against malicious usage and in general, follows UF Procedures to Develop Applications for Secure Deployment.

## **Change Management Standard**

Changes to IT resources must be planned, documented and announced to the appropriate audience. The planning must consider the impact on confidentiality, integrity, availability, recoverability and auditability.

## **Other Standards**

### **OIT Standard: Private IP**

[http://net-services.ufl.edu/network\\_information/documents/private-ip.html](http://net-services.ufl.edu/network_information/documents/private-ip.html)

### **Secure Build Best Practices**

<http://infosec.ufl.edu/admins/build.shtml>

### **OIT Standards - SMB Filter**

<http://infosec.ufl.edu/admins/smb-std.shtml>

### **OIT Standards - Dialup/WIPA SMB Filter**

<http://infosec.ufl.edu/admins/smb-dialup.shtml>

### **OIT Standards - MS SQL Filter**

<http://infosec.ufl.edu/admins/mssql-std.shtml>

### **OIT Standard - Authorized Email Flow**

<http://infosec.ufl.edu/admins/email-std.shtml>

### **OIT Standard: DHCP IP Network Number Distribution**

[http://net-services.ufl.edu/network\\_information/documents/ip-distribution.html](http://net-services.ufl.edu/network_information/documents/ip-distribution.html)

This page intentionally left blank

# UF IT Security Incident Response Standard

The UF Incident Response Team (UFIRT) is led by the UF ISM. UFIRT is composed of IT security staff reporting to the UF ISM, and others as appropriate for the incident. UFIRT assesses threats to UF IT resources, determines vulnerabilities of UF IT resources, processes IT security complaints, and detects and tracks UF network IT security incidents. UFIRT has primary authority in response decisions for incidents that impact UF mission critical services.

Unit incident response teams are led by the Level 2 Unit ISM and composed of unit IT workers listed in the Network Services contact database and others as appropriate to the incident.

The following incident types require a response:

- Incidents involving threat or damage to property or people
- Child pornography
- IT Resource vulnerabilities
- Compromise
- AUP violation

All UF and subsidiary units must immediately notify the UFIRT of security incidents in their unit involving:

- Threats to other IT resources.

UF and applicable subsidiary Level 2 Unit ISMs must immediately notify the UFIRT of security incidents in their unit involving:

- Copyright violations
- Unauthorized privileged access

UF and applicable subsidiary Level 2 Unit ISMs should consult with the UF General Counsel to determine if law enforcement should be notified. Law enforcement should be notified of incidents involving:

- Threats to property or life
- Damages in excess of \$10,000
- Child pornography

Other incidents should be reported according to the judgment of the Level 2 Unit ISM.

## Critical IT Resources Standard

A critical IT resource is vital to the function of the unit. It might store sensitive data, confidential data, or data protected by law. Systems classified as critical IT resources must meet the minimum standards of a production server as defined in UF Network and Host Security Standard. Critical IT resources may need special consideration with respect to risk assessment, service interruption, and notification. To be registered, critical IT resources must have IT personnel resources available 24 hours per day, 7 days per week.

## Procedures to Register Critical IT Resources

Level 2 Unit ISMs can submit a written request to register critical IT resources with the UF ISM. All submissions for classification as a critical IT resource will be reviewed by the ITAC-ISM and considered for approval by the UF ISM. An incident response plan must be filed with the UF ISM describing risk assessment, service interruption, and notification procedures.

## Service Interruption Notification Procedures

Level 2 Unit ISMs will be notified prior to or concurrent with a service interruption applied as the result of a security incident. Notification attempts will be made to Level 2 Unit ISMs and/or network managers, or their designees, directly by phone, beeper, or email, in that order. Accordingly, notification may be made by way of **net-managers-l@lists.ufl.edu** when multiple hosts from varied networks are affected. An effort will be made to avoid disruption of service in cases not involving outgoing attacks.

## Incident Response Procedures for Vulnerabilities

Examples: patch or upgrade needed, weak password, unrestricted access

1. Discovery. The UF Incident Response Team assesses threats of UF IT resources. When a threat is discovered, it is documented and IT workers are alerted. When possible, UF IT resources are assessed for vulnerability to the threat and appropriate contacts are notified. Level 2 Unit ISMs must ensure vulnerability and threat assessment within their unit. A vulnerability scanner is available to authorized UF network and server administrators at <https://infosec.ufl.edu/admins/scans.shtml>.

2. Notification. When a vulnerability is discovered by the UF Incident Response Team, appropriate contacts are notified and the incident is documented in the UF incident tracking system. Contacts are identified using the UF Network Services subnet and domain contact resources. The Level 2 Unit ISM will be copied on all notifications. Follow the URL in the notification to a form that is to be used for entering updates about the incident. If no URL is provided, contacts must respond to the original notification, including content of the original notification, to acknowledge receipt, containment and commencement of the investigation.

3. Resolution. Common resolutions to correct a vulnerability are upgrading and patching. Alternatives include physical, network, host, user and/or other access restrictions. Other resolutions may also apply. When resolved, follow the URL in the notification to a form that is to be used for entering updates about the incident. If no URL is provided, contacts must respond to the original notification, including content of the original notification, to acknowledge resolution.

# Incident Response Procedures for Compromised IT Resources

Examples: attack/exploit, backdoor or trojan, denial of service, malware, unauthorized access

1. Discovery. UFIRT receives and processes discovery notifications from other sources. UFIRT manages systems to discover incidents that cross core boundaries on the UF network. Units are responsible to deploy systems to detect incidents behind core boundaries as needed.

2. Documentation. The UFIRT documents UF IT security incidents in a tracking system. Units should track incidents in their own tracking system. Recommendations for tracking systems include RTIR , GNATS, or SANS.

The Level 2 Unit ISM retains a detailed log, including accurate times, maintained during the incident. The Level 2 Unit ISM ensures preparation of a summary of the incident for:

- the Level 2 Unit ISA,
- affected Data Principals and
- other relevant management.

The following information should be included in the summary:

- How the incident was detected
  - Dates
    - Inferred date of compromise
    - Date the compromise was detected
    - Date the incident was finally resolved
  - Names
    - People added to the Unit Incident Response Team for this incident
    - Person responsible for the IT Resource
    - Person compromising the resource, if known
  - Scope
    - Cause of the vulnerability
    - Impact of the incident
    - Nature of the resolution
  - Proposed improvements

The summary for management will probably contain sensitive information and in any case would not be targeted at the user community. Where appropriate, the Level 2 Unit ISM should also prepare an incident summary for the users, using the incident as an object lesson to reinforce safe practices.

3. Notification. Contacts for incidents detected by UFIRT are identified using the UF Network Services subnet and domain contact resources (<https://net-services.ufl.edu/ns/cgi-bin/subnet-form.cgi>). The UFIRT notifications may be augmented as needed to include staff with appropriate knowledge and skills. Appropriate contacts are notified and recorded in the tracking system. The

## UF Information Technology Security Regulations

Level 2 Unit ISM will be copied on all notifications. Follow the URL in the notification to a form that is to be used for entering updates about the incident. If no URL is provided, contacts must respond to the original notification, including content of the original notification, to acknowledge receipt, containment and commencement of the investigation.

All UF and subsidiary units must immediately notify the UFIRT of security incidents in any unit involving threats to other IT resources, unauthorized privileged access, or incidents involving law enforcement.

If one UF unit becomes aware of a compromised IT resource in another UF unit, the manager of the network containing the compromised machine should be notified, and the UFIRT and the Level 2 ISM for that unit should be copied. Network manager contact information is maintained by UF Network Services (<https://net-services.ufl.edu/ns/cgi-bin/subnet-form.cgi>).

UFIRT notifications should be acknowledged immediately, but no later than 24 hours after they are sent.

4. Containment. UF IT resources engaged in active attacks against other IT resources must be contained immediately. Unless further investigation requires unrestricted access, all other incidents must be contained as soon as possible, but no later than the same business day in which the notification is received.

Containment can be achieved by immediately disconnecting the resource from the network, revoking user access, or other means as appropriate. Unit IT workers may coordinate with the UFIRT to restrict access to compromised hosts that can't be immediately disconnected or must remain connected in a restricted environment for the purpose investigation or providing service. UFIRT has the authority to coordinate with Network Services to block compromised services and/or hosts that present a definitive danger to the rest of the network. Notification will follow the procedures outlined in the Service Interruption Notification section above.

5. Investigation. Investigation includes analysis, identification, prioritization, and evidence collection and retention.

- Analysis. Compromised hosts must be assessed.
  - <http://sans.org/resources/winsacheatsheet.pdf>
  - [http://www.sans.org/score/checklists/ID\\_Windows.pdf](http://www.sans.org/score/checklists/ID_Windows.pdf)
  - [http://www.sans.org/score/checklists/ID\\_Linux.pdf](http://www.sans.org/score/checklists/ID_Linux.pdf)
- Identification. Identify source as appropriate, including user, host or other resource.
- Severity Assessment. Determine criticality of resource and impact on other resources.
  - Does law enforcement need to be notified?
  - Is there an immediate impact to UF or unit mission critical services?
  - Is there potential impact to UF or unit mission critical services?
  - Does the incident impact the local host only?
- Evidence Collection and Retention. If the method of compromise is unique or cannot be determined, or if forensics evidence is needed for law enforcement, an image of the compromised hosts must be retained. Email and any other relevant evidence must also be retained.

6. Resolution. Incidents must be resolved as soon as possible, preferably the day of the notification, but no later than noon on Friday of the same week. Compromised hosts must be reformatted, rebuilt and

## UF Information Technology Security Regulations

have vulnerabilities resolved before reconnecting them to the network. However, at the discretion of the UF ISM, in consultation with the Level 2 Unit ISM, compromised hosts may be cleaned and patched expeditiously. Incidents must be resolved to the satisfaction of the UFIRT before compromised hosts are reconnected to the network or filters are lifted. In some cases, the UFIRT may request privileged access to ensure the host is safe to resume network connectivity, or may require that it be evaluated for vulnerabilities before being placed back in service. Follow the URL in the notification to a form that is to be used for entering updates about the incident. If no URL is provided, contacts must respond to the original notification, including content of the original notification, to acknowledge resolution of the investigation.

The IT workers responsible for the IT Resource that has been compromised must distribute to impacted users and their supervisors a user-oriented summary of the incident including:

- Impact on the user's work
- Remediation or preventative measures the users should take

In particular, if passwords have been compromised, they must be reset and changed by the users, once the system has been secured.

# Incident Response Procedures for Copyright Infringement

Examples: movies, music, unlicensed software and other intellectual property.

## Initial Notice

Any formal Digital Millennium Copyright Act (DMCA) complaints received directly from a representative of the copyright holder should be referred to UF's designated agent for DMCA complaints (dmca@ufl.edu). Non-DMCA complaints (complaints not intended to conform to the requirements of the DMCA) should be resolved by the Level 2 Unit ISA and Unit ISM if possible. If not easily resolved, forward non-DMCA complaints to dmca@ufl.edu.

Upon receipt of a complaint, UF's DMCA agent will examine the notice of copyright infringement to determine whether it contains the elements required by the DMCA.

- Identification of the copyrighted work claimed to have been infringed.
- Identification of the material that is claimed to be infringing and that is to be taken down or disabled, and information "reasonably sufficient" to enable the service provider to locate the materials.
- Information "reasonably sufficient" to enable the service provider to contact the complainant.
- A physical or electronic signature of a person authorized to act on behalf of the owner (i.e., the copyright owner or its licensee) of the right that is alleged to be infringed.
- A statement that the complainant has "a good faith belief" that use of the material in the manner complained of is not authorized by the copyright owner, the owner's agent, or the law.
- A statement that the information in the notification is accurate and that, under penalty of perjury, the complainant is authorized to act on behalf of the copyright owner.

## Action Upon Receipt of Notice

If the notice substantially complies with A, B, and C above, UF's DMCA agent will forward the complaint to the appropriate IT worker and the Level 2 Unit ISM as listed in the UF Network Services contact list (<https://net-services.ufl.edu/ns/cgi-bin/subnet-form.cgi>) and send a copy to dmca@ufl.edu.

If the complaint complies with A, B, and C, but does not substantially comply with D, E, and F, more information may be requested from the complainant. Only if the notice does not adequately comply with A, B, and C above or if the complainant does not respond to request for more information can the UF DMCA agent disregard the notice.

## UF Information Technology Security Regulations

The procedures listed below must be followed upon receipt of a notice of copyright violation from the UF DMCA Agent:

- The Level 2 Unit ISM will ensure that public access to the material targeted by the complaint is disabled as quickly as reasonably possible. If after one business day this action has not been taken, the UF DMCA agent will request that UF Network Services block access to the material.
- The Level 2 Unit ISM will ensure that the person believed to be responsible for the alleged infringing distribution of copyrighted material is notified of the complaint, and of the action taken to remove access to the material. The person must be given an opportunity to contest the removal of the material if they believe the complainant has misidentified it or if the material is lawful. If they choose to contest the removal, follow the procedure Counter-Notification procedures below.
- If the material in question is not legally possessed by the person believed responsible for making it publicly accessible, the Level 2 Unit ISM will ensure that the material is removed from the system on which it was found.
- The Level 2 Unit ISM will ensure that the UF DMCA agent is notified when the material is no longer publicly accessible, and that the UF DMCA agent is notified if the person responsible for distributing the material is contesting its removal.
- If the person responsible for distributing the material is a student, forward the matter to the Office of Student Judicial Affairs. If the person is an employee, notify the appropriate Dean, Director, or Department Chair.

### **Counter-Notification**

If the person responsible for the alleged infringing distribution of copyrighted material believes the material was misidentified or the distribution was lawful, they should send a counter-notification to the UF DMCA agent. The counter-notification must contain the following:

- A physical or electronic signature of the person responsible for the alleged infringing distribution.  
Identification of the material (or the location of the material) to which public access has been disabled. The identification should match the original identification provided by the complainant.
- A statement under penalty of perjury that the alleged infringer has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material.
- The alleged infringer's name, address and telephone number, and a statement that the alleged infringer consents to the jurisdiction of the federal district court for the judicial district in which the alleged infringer is located and that the alleged infringer will accept service of process from the complainant.

The UF DMCA agent should work with the alleged infringer to obtain any missing components of the counter-notification. When the counter-notification is complete, the UF DMCA agent will forward it to the complainant, along with a notification that the removed material may be restored in ten business days unless legal action is commenced against the alleged infringer.

If the complainant fails to notify the UF DMCA agent that it has initiated legal proceedings within ten business days after receiving a counter-notification, the UF DMCA agent will notify the Level 2 Unit ISM that the material may be returned to public distribution.

## **Response Procedures for Incidents Involving Law Enforcement**

Examples: obscenity, stalking, threat of bodily harm, child pornography, unauthorized access.

Law enforcement should be notified of incidents involving threat to property or life, damages in excess of \$10,000, or child pornography. UF and applicable subsidiary Level 2 Unit ISMs should consult with the Level 2 Unit ISA and the UF Office of General Counsel (OGC) to determine if law enforcement should be notified. Other incidents should be reported according to the judgment of the Level 2 Unit ISM.

When incidents involve law enforcement, contact the University Police Department (UPD) and the OGC. Secure evidence without reviewing additional content. If the incident involves a student, notify Student Judicial Affairs (SJA). If the incident involves an employee, notify the appropriate Dean, Director or Department Head.

Network hardware, software or data may be considered evidence. Care must be taken to preserve evidence. A public records request, subpoena, warrant or other official request must be issued before data is released to law enforcement. Contact OGC to review public records requests, subpoenas, and warrants before responding. Evidence from incidents that involve an immediate threat to property or life may be provided to law enforcement in advance of a public records request, subpoena or warrant, but OGC should be contacted if time allows.

## **Incident Response for Non-criminal, Legal Issues**

Examples: defamation, civil fraud.

Secure evidence without reviewing additional content. Contact the Office of the General Counsel.

## **Incident Response Procedures for Violations of the UF Acceptable Use of Computing Resources policy (AUP)**

Examples: excessive or disruptive use, complaint, spam, inappropriate content, suspicious activity,

IT workers that identify violations of the UF Acceptable Use of Computing Resources policy should take action as reasonably necessary to protect UF and IT resources, and notify the violator of the action. For disciplinary action, notify Student Judicial Affairs if the violator is a student, or notify the Dean, Director, or Department Chair if the violator is an employee. IT workers do not make disciplinary decisions unless they supervise the violator. In all events, follow UF disciplinary procedures defined by UF Human Resources.

## **Incident Response Procedures for Sexual Harassment**

Secure evidence without reviewing additional content. Contact the appropriate Dean, Director, or Department Chair; Office of the General Counsel; and Associate Provost for Affirmative Action.

## **Incident Response Procedures for Allegations of Americans with Disabilities Act (ADA) Violation**

Examples: no disabled access to computers, software or web sites

If incident cannot be easily resolved, refer complaint to the Office of the General Counsel and the ADA Compliance Office.

This page intentionally left blank

# UF IT Security Physical Security Standard

Physical IT resources include offices, hardware, IT documentation, and other tangible assets. To protect their confidentiality, integrity, and availability, physical IT resources must not be accessible without authorization.

It is the responsibility of all UF and subsidiary units to identify and document all UF IT resources to be protected.

The Level 2 Unit ISM is responsible for the protection of all IT infrastructure, equipment, and hardware located within their unit. The Level 2 Unit ISM must document adequate physical security measures for the protection of physical and logical assets, and sensitive applications and data.

Level 2 Unit ISM must ensure identification, documentation, and implementation of auditable locks where necessary to secure IT resources in their unit. Where appropriate, campus locations must coordinate with Physical Plant Division (PPD), 392-1411. Where possible, IT resources should be aggregated to reduce the cost of physical security and environmental control.

## UF Physical Security Procedures

Physical access to servers and network equipment should be limited to authorized individuals. Network cables should be organized, labeled, and protected from interference. Network documentation must be maintained to identify network jack location. Reasonable methods should be used to physically secure ports. These include but are not limited to locking offices and disabling inactive switch ports. See the following documents for more information:

- University of Florida Handbook on Business Policies and Procedures
- UF Telecommunications Construction Standards
- Network Services labeling documentation

This page intentionally left blank

# UF IT Security Risk Assessment Standard

The UF ISM will conduct a comprehensive risk analysis of security threats to IT resources for selected UF units at least once every three years.

The Level 2 Unit ISM must ensure that IT risk assessments are performed for their unit at least annually. The purpose is to determine protection level commensurate with resource value and exposure to threats. The standard risk assessment includes:

- Asset inventory
- Documentation update (inventory services)
- Accounts and access privileges audit
- Software licenses audit
- Positions of Special Trust agreements audit
- Data security roles and classifications
- Awareness program audit
- Review and update of policies, standards, and procedures
- Policies, standards, and procedures compliance audit
- Network access control audit
- Port scans (where applicable)
- Vulnerability scans (where applicable)
- Anti-malware protection
- IT Continuance of Operations Plan

## UF Risk Assessment Procedures

The UF Incident Response Team (UFIRT) conducts port scans to identify common services and other services of interest every Monday starting at 4:00 am. Authorized network contacts identified using the UF Network Services subnet and domain contact resources can access results of the weekly port scans from the Network Manager Security Data web site.

Vulnerability scans are conducted as needed to assess UF risk to specific active threats. Unit ISMs and network contacts will be notified of new scans of their network via direct email or the net-managers-l@lists.ufl.edu listserv. Effort will be made to notify them prior to the scan as circumstances allow. It is a violation of UF policy to knowingly and intentionally subvert risk assessment. Unit ISMs and network contacts are notified immediately by email of vulnerabilities, but they may also access results from the Network Manager Security Data web site. Based on the vulnerability results, Level 2 Unit ISMs must ensure that measures are taken to address security weaknesses. The UF Incident Response Team (UFIRT) may apply preemptively block vulnerable hosts identified through vulnerability scans. Notification regarding service disruption will follow the procedures outlined in the Service Disruption Notification section of the Network and Host Security Standard.

Network contacts may schedule port and vulnerability scans of networks for which they are authorized from the Network Manager Security Data web site. All UF and subsidiary units are encouraged to conduct their own port and vulnerability scans, but to avoid being misinterpreted as an attack, prior notification of all probes must be sent to net-services@ufl.edu.

This page intentionally left blank

# UF IT Security Training and Awareness Standard

Level 2 Unit ISMs have the following responsibilities regarding training and awareness in their units:

- They must ensure that all users within their unit are aware of, have access to, and comply with the UF Acceptable Use Policy.
- They must ensure that all people who maintain or manage IT resources within their unit are aware of, have access to, and comply with their unit's and UF's information technology security policies, standards, and procedures.
- The Level 2 Unit ISM must ensure that all IT workers in their unit receive UF IT Orientation before their probationary period ends.

## Training and Security Awareness Procedures

IT staff of UF and applicable subsidiary units are required to attend orientation to inform them of available resources and their responsibility to comply with University policies. Subsidiary units must supply their IT staff with orientation materials agreed upon by the UF ISM and the Unit ISM. IT staff are encouraged to attend Information Technology Security Awareness Day and other security training offered on site at UF.

This page intentionally left blank

# UF IT Security Continuance of Operations Standard

The Level 2 Unit ISM must ensure that their unit maintains an Information Technology Continuance of Operations Plan (ITCOP). There must be written plans detailing procedures for various disaster scenarios, both natural and man made. To guard against disaster, critical IT resources must be preserved against loss or corruption by appropriate backup procedures.

The Level 2 Unit ISA has the responsibility to coordinate with the campus emergency response team as appropriate regarding preparation and recovery from incidents.

## Continuance of Operations Guidelines

University of Florida units are required to maintain a written IT Continuance of Operations Plan (ITCOP). This document is intended as a guideline to help simplify the development of a Unit ITCOP.

Since the ITCOP contains sensitive information about unit IT resources, the plan should not be advertised, but it must be made available to the UF ISM upon request.

Include the unit name in the plan title. Identify the network managers, the unit administrator and list their contact information.

It is not necessary that units include everything listed here, but they should include those things that are relevant to IT functions of their unit.

## Components of ITCOP

Cover Sheet: identification, dates, locations, disclosure statement

Overview: executive summary, policies, concepts

Introduction: purpose, goals, objectives, benefits

Scope: what IT resources does the ITCOP address

Contacts and Responsibilities

Resources: documentation

Risk assessment: value, criticality, threats, replacement costs, acceptable downtimes

Preparation: monitoring, backups, training, testing

Recovery: what constitutes a disruption, procedures

Revisions: environmental changes, test results, revision schedule

## **ITCOP cover sheet**

- Unit name
- Unit ISM
- Unit ISA
- Date Established
- Date of Last Revision
- Distribution list
- Locations of document
- Sensitive Information Disclosure Notice

## **Overview**

- Executive management perspective
- Policies
- Plan concepts
- What constitutes a disruption
- Summary of ITCOP

## **Introduction**

- Purpose
- Goals
- Objectives
- Benefits

## **Scope**

- IT resources addresses by ITCOP

## **Contacts and Responsibilities**

- ITCOP Activation Authority
- ITCOP Coordinator
- Resource contact(s)
- Alerting/monitoring contact(s)
- Training contact(s)
- Testing contact(s)
- Update contact(s)
- PPD/Facilities contact
- Emergency Building Coordinator contact
- UPD contact
- Key management contact
- Other physical security contacts
- Other contacts

## **Resources**

Resource types

People

Data

Equipment and hardware

Software

Processes

Service Providers

Buildings and Facilities

Resource documentation details

Location

Description

Value

Criticality

Resource considerations

Data backups

Power backups, batteries and generators

Replacement resources

Warranty records

Maintenance contracts

Vendor managed resources

Environmental controls

## **Risk assessment**

Prioritize IT resources

Assess the value and criticality of IT resources

Determine threat to IT resources

Assess cost to replace IT resources

Determine acceptable downtime of IT resources

## **Preparation**

Alerting/monitoring

Maintenance contracts that need to be maintained

Data backup procedures

- Location

- Frequency

- Incremental vs. full

- What is backed up

Privileged passwords maintenance and recovery

Power backups

Training

- Team

- Scope

- Schedule

- Procedures

Testing

- Team

- Scenario

- Schedule

- Monitoring

- Follow-up

**Recovery:** A prioritized business resumption task list based on type of event (facilities, personnel, IT services, IT equipment failures or loss). What needs to be done (damage assessment, notification procedures, ITCOP activation), when, where, and how.

1. Establish communication
2. Notification
  - Internal personnel
  - Network Services
  - Network Managers
  - PPD
  - UPD
  - EHS
  - State insurance
3. Damage assessment and documentation
  - Photograph scene untouched to document smoke, water, or other damage
  - Outsource forensics services if needed
4. Establish basic services
  - Networking
  - Restore backups
  - Relocate equipment
5. Replacements
  - Building and facilities
  - Staff
  - Equipment
  - Keys
  - Tools
6. Cleanup
  - PPD
7. Resumption of services
  - Full resumption
  - Alternative manual methods for operation
8. Establish communication
  - Phones - forwarding numbers and other configuration options
  - Email - establish alternative email accounts for key contact personnel

### **Revisions**

- Consider equipment and environmental changes
- Consider test results
- Establish revision schedule

