
Incident Response Plan

**Office of Information and
Instructional Technology**

USG Sensitive
January 03

SENSITIVITY NOTICE

University System of Georgia (USG) - Sensitive

This security report is classified as USG sensitive. It contains sensitive system security information relating to the security services, processes, and operations of the USG enterprise information network. Unrestricted public disclosure of this information would assist unauthorized persons to breach the USG educational network systems and place 'privacy' and other sensitive categories of information at risk.

Contents

1	INTRODUCTION.....	1
1.1	PURPOSE	1
1.2	RESPONSE TEAMS	1
2	INCIDENTS	3
2.1	SEVERITY LEVELS.....	3
3	INCIDENT RESPONSE	5
3.1	ORGANIZATION.....	5
3.2	THE INCIDENT RESPONSE PROCESS.....	6
3.2.1	<i>Defining Severity Levels</i>	6
3.2.2	<i>Responding to Incidents</i>	7
3.2.3	<i>Following-Up</i>	10
4	APPENDIX.....	11

1 Introduction

This document provides a general framework to illustrate how each institution and the Board of Regents, Office of Information and Instructional Technology (OIIT) can coordinate responses to major security incidents. There are basic components, procedures, and general guidelines for dealing with computer security incidents that are applicable to all organizations. Through these mechanisms the University System of Georgia (USG) can minimize security vulnerabilities and respond to security incidents in an efficient manner that is critical to business continuity.

1.1 Purpose

The purpose of the Incident Response Plan is to combine needed resources in an organized manner to address adverse incidents related to the safety and security of a USG technology resource. We recommend that each campus develop an Incident Response Plan to address adverse incidents such as:

- Malicious code attack
- Unauthorized access to USG systems
- Unauthorized utilization of USG services
- Denial of service attacks (DOS)
- General misuse of systems
- Hoaxes

1.2 Response Teams

As part of this plan, it is recommended that each campus create a local Computer Incident Response Team (CIRT). As a complement to each CIRT, the newly established OIIT Computer Incident Coordination Team (CICT) will provide additional resources and services for major security incidents.

Incident Response Report

The general purpose and objectives of the CIRT and CICT are as follows:

Team	Purpose	Objectives
CIRT	<ul style="list-style-type: none"> • Protect the institutions information and technology assets • Create a central organization to handle incidents • Comply with government or other regulations • Prevent the use of local institutional systems in attacks against other systems that could result in legal liability • Minimize the potential for negative exposure 	<ul style="list-style-type: none"> • Limit immediate incident impact to the institution • Recover from the incident • Determine how the incident occurred and attempt to determine the origin • Determine how to avoid further exploitation of the same vulnerability • Avoid escalation and further incidents • Assess the impact and damage • Update campus policies and/or procedures as needed
CICT	<ul style="list-style-type: none"> • Assist the local CIRT in protecting the institution's Information Technology (IT) assets • Provide a central organization to handle high level incidents • Assist the local CIRT in complying with government or other regulations • Help minimize the potential for negative exposure 	<ul style="list-style-type: none"> • Provide additional resources to limit immediate incident impact to the institution • Assist the institutions in recovering from an incident • Help determine how the incident occurred and determine the origin of the incident if possible • Provide recommendations to avoid further exploitation of the same vulnerability • Assess the impact and damage • Provide recommendations to update campus policies and/or procedures • Coordinate the distribution of information to other institutions as necessary to limit the potential risk and/or propagation of a threat

2 Incidents

An incident is any occurrence that poses a threat to sensitive data in the campus network. Sensitive data is defined as follows:

- Student data protected by the Family Educational Rights and Privacy Act (FERPA)
- Patient data/medical records protected by the Health Insurance Portability and Accountability Act (HIPAA)
- Social security numbers
- Credit card and other financial data
- Sensitive research data

2.1 Severity Levels

Incidents are categorized at one of three severity levels based on the impact to the campus and USG as a whole. The following table provides general definitions and description of each severity level:

Severity Level	Definition	Examples
High	Incidents that have a severe impact on the institution's business or services	<ul style="list-style-type: none"> • Malicious code attacks • Unauthorized access • DOS affecting the entire campus • Compromise of host with sensitive data
Medium	Incidents that have a significant impact, or the potential to have a severe impact on the institution's business or services	<ul style="list-style-type: none"> • Attempts to gain unauthorized access • DOS attack affecting a building/department • Open mail relay on campus
Low	Incidents that have a minimal impact with the potential for significant or severe impact on the institutions business or services	<ul style="list-style-type: none"> • Unauthorized network probes or system scans • Isolated virus infections

3 Incident Response

Responding effectively to incidents requires policies and procedures observed by all parties, and an organization of trained personnel who can respond as necessary. This section describes these aspects of incident response.

In general, there are seven recognized stages of incident response:

Stage	Definition
Preparation	Prepare a response plan and train the appropriate personnel to respond when necessary. The most important aspect of a response plan is the ability to actively adhere to its contents once it is in place. Knowing how to respond to an incident before it occurs can save valuable time and effort in the long run. Refer to the Board of Regents policy 712.03 D for more information.
Identification	Determine if an incident has occurred and identify the nature of it.
Reporting	Inform the appropriate parties and groups in case of an incident. It is very important that campus officials are aware of any incident occurring on a campus.
Containment	Attempt to limit the scope and magnitude of the incident. Many incidents involve malicious code that can spread rapidly. Immediate containment is vital.
Eradication	Remove or mitigate the factor(s) that caused the incident. This is a crucial element of the response plan, despite the difficulties in carrying it out.
Recovery	Restore the system to normal business status. Once a restore has been performed it is also important to verify the restore operation was successful and that the system is back to its normal condition.
Follow-up	Identify areas in the response plan that can be improved and implement new policies and procedures as necessary. The main goal is to learn from the incident and follow-up activities are a valuable part of the process.

3.1 Organization

To adequately respond to an incident, pre-determined teams will respond depending on incident characteristics. As the situation develops and the impact becomes more significant, various other teams will be called to contribute. *Figure 1* depicts the OIIT CICT team structure:

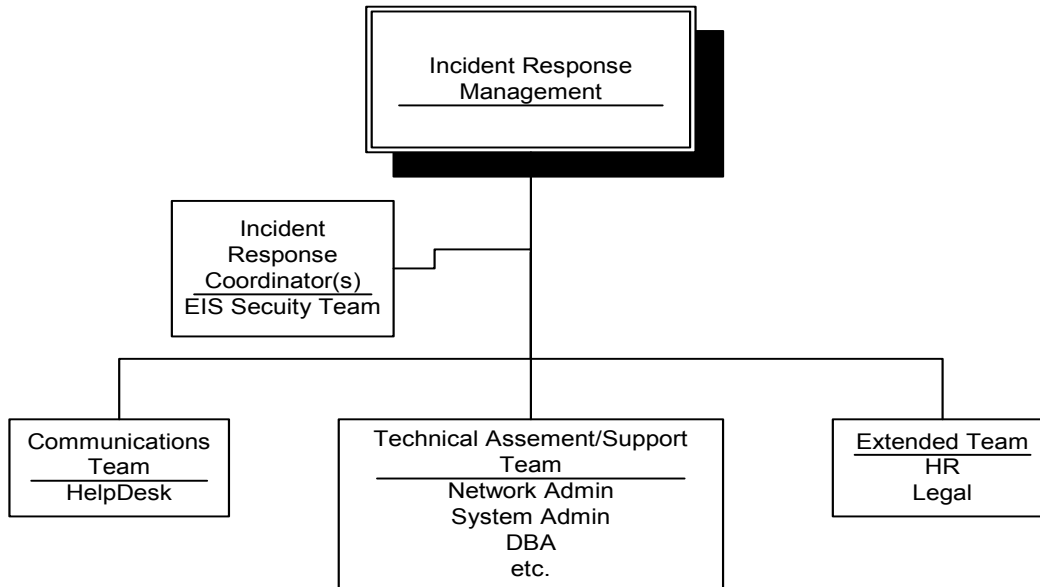


Figure 1: Incident response organization. This structure can also serve as a model for a local Incident Response Team.

3.2 The Incident Response Process

The process outlined below illustrates how an individual campus and the OIIT can work together, when appropriate, to ensure a security incident is assessed and that required resources are brought to bear on the problem based on the severity level. In the event the incident becomes more widespread or an escalated response due to an increased level of severity is required, team members at the next highest level will be placed on alert.

Note: Each institution may have unique organizational structures. However, for the purpose of the defined responses below, the organizational structure illustrated in *Figure 1* will be used as the model.

3.2.1 Defining Severity Levels

It is important to identify the severity level before responding to an incident. Severity levels are defined in section 3.2.2. The Incident Response Management Team is responsible for characterizing the incident in order to determine the severity. Factors to consider include but are not limited to the following:

- How widespread is the incident?
- What is the impact to the institution's production operations?
- How difficult is it to contain the incident?
- How fast is the incident propagating?
- Has sensitive data been compromised?
- Has compliance with state and federal regulations been threatened?
- Will this negatively affect the image of the institution or the USG?

3.2.2 Responding to Incidents

This section outlines the roles and responsibilities of the response teams. Refer to 3.1 in this report for more information about the OIIT CICT team organization. We recommend that each institution monitor all known sources for alerts or notification of a threat. Internal sources include firewalls, ISS, and log files. Refer to the Appendix for more information about external sources.

The following table defines the roles and responsibilities of the security organization, depending on the severity of the incident. Refer to 2.1 in this report for descriptions of each severity level.

Severity Level	Actor	Action
Low	CIRT	<ol style="list-style-type: none"> 1. Determine initial defensive action. 2. Notify the local Incident Coordinator. 3. Notify the appropriate support organization if an action, such as updating anti-virus files, is necessary.
	Local Incident Coordinator	<ol style="list-style-type: none"> 1. Receive and track all reported potential threats. 2. Determine relevant membership of the Technical Assessment/Support team. 3. Alert local and applicable support organizations and of the potential threat and any defensive action required. 4. Alert local Incident Response Management of the potential threat. 5. Alert the local Communications team.
	Local Communications Team	Notify employees regarding any necessary required action.

Incident Response Report

Severity Level	Actor	Action
Medium	Incident Response Management	<ol style="list-style-type: none"> 1. Assume responsibility for directing response activities to the incident. 2. Direct the local Incident Response Coordinator to: <ul style="list-style-type: none"> • Set up communications between all Incident Response team managers and technical support team in the field. • Request additional support services from OIIT CICT if necessary. 3. Alert the Extended Team and notify them of the security level, if necessary. 4. Determine when the risk has been mitigated to an acceptable level.
	Local Incident Response Coordinator	Maintain a chronological log of events.
	Technical Assessment/Support Team	<ol style="list-style-type: none"> 1. Determine and implement the best course of action for containment of the incident. 2. Monitor all known sources for alerts for further information or actions to take to eliminate the threat. 3. Report the status to the local Incident Response Coordinator for the chronological log of events. 4. Monitor effectiveness of actions taken and modify them as necessary. 5. Notify the local Incident Response Coordinator of effectiveness of actions taken and progress in eliminating the threat. 6. Implement actions to eradicate the threat as directed by the Incident Response Management and/or Incident Response Coordinator.
	Extended Team	<ol style="list-style-type: none"> 1. Contact local authorities if necessary. 2. Arrange for local authorities to access appropriate facilities and resources if necessary. 3. Ensure that all necessary information is collected to support any possible legal or personnel action.
	Communication Team	Communicate with the institutional population as directed by Incident Response Management.

Severity Level	Actor	Action
High	Incident Response Management	<ol style="list-style-type: none"> 1. Assume responsibility for directing response activities to the incident. 2. Direct the local Incident Response Coordinator to: <ul style="list-style-type: none"> • Set up communications between all Incident Response team managers and technical support team in the field. • Limit the potential scope of the incident by notifying OIIT CICT. Make this notification as quickly as possible and provide follow-up information as the incident develops. Refer to the Appendix for contact information. • Request additional support services from OIIT CICT if necessary. 3. Alert the Extended Team and notify them of the security level, if necessary. 4. Provide status reports to the campus executive management and OIIT management as appropriate. 5. Determine when the risk has been mitigated to an acceptable level.
	Local Incident Response Coordinator	<ol style="list-style-type: none"> 1. Maintain a chronological log of events. 2. Provide numbered status reports to appropriate management structures and the OIIT CICT.
	Technical Assessment/Support Team	<ol style="list-style-type: none"> 1. Determine and implement the best course of action for containment of the incident. 2. Monitor all known sources for alerts and look for further information or actions to take to eliminate the threat. 3. Report the status of the incident to the local Incident Response Coordinator as well as the chronological log of events. 4. Monitor effectiveness of actions taken and modify them as necessary. 5. Notify the local Incident Response Coordinator about the effectiveness of actions taken and the progress in eliminating the threat. 6. Take action to eradicate the threat as directed by Incident Response Management and the Incident Response Coordinator.
	Extended Team	<ol style="list-style-type: none"> 1. Contact local authorities if necessary. 2. Arrange for local authorities to access facilities and resources if necessary. 3. Ensure that all necessary information is collected to support any possible legal or personnel actions.
	Communication Team	Communicate with the institutional population as directed by Incident Response Management.

3.2.3 Following-Up

The follow-up stage of incident response is outlined in the following table:

Severity Level	Actor	Action
Low and Medium	Incident Response Management	<ol style="list-style-type: none"> 1. Prepare a report for institutional executive management that includes: <ul style="list-style-type: none"> • Estimates of damage/impact • Action taken during the incident (not technical detail) • Follow-up on efforts needed to eliminate or mitigate the vulnerability • Policies or procedures that require updating • Efforts taken to minimize liabilities or negative exposure 2. Provide the chronological log and any system audit logs requested by the Extended Team. 3. Document lessons learned and modify the Incident Response Plan accordingly.
High	Incident Response Management	<ol style="list-style-type: none"> 1. Prepare a report for institutional executive management that includes: <ul style="list-style-type: none"> • Estimates of damage/impact • Action taken during the incident (not technical detail) • Follow-up on efforts needed to eliminate or mitigate the vulnerability • Policies or procedures that require updating • Efforts taken to minimize liabilities or negative exposure 2. Provide the chronological log and any system audit logs requested by the Extended Team. 3. Document lessons learned and modify the Incident Response Plan accordingly.
	Extended Team	<ol style="list-style-type: none"> 1. Conduct legal work with local authorities as appropriate. 2. Consult with management, Human Resources, and Institution Security to determine disciplinary action as appropriate.

4 Appendix

The following is a list of alert or notification resources:

Resource	Contents
ASSIST www.microtech.doe.gov/ASSIST/index.html	Automated Systems Security Incident Support Team
BUGTRAQ www.securityfocus.com	Information on UNIX related security holes/backdoors (past and present) that include: <ul style="list-style-type: none"> • Exploit programs • Scripts and detailed processes • Patches, fixes, and known workarounds • Ideas, future plans, or current processes dealing with UNIX security information material regarding vendor contacts and procedures • Individual experiences in dealing with above vendors or security organizations • Incident advisories or informational reporting
CERT www.cert.org	In response to computer security threats, the Advanced Research Projects Agency (ARPA) established the Computer Emergency Response Team (CET) coordination center to support Internet users.
CERT-NL cert.surfnet.nl/home-eng.html	CERT-NL is the SURFnet Computer Emergency Response Team that handles computer and network security incidents related to hacking, vulnerabilities, and viruses.
CIAC www.ciac.org/cgi-bin/index/bulletins	The U.S. Department of Energy's Computer Incident Advisory Capability established in 1989. CIAC provides computer security services to employees and contractors of the Department of Energy.
Hewlett Packard Security Bulletins itrc.hp.com	Security bulletins relevant to Hewlett Packard products and systems.
Sun Microsystems sunsolve.sun.com	Security advisories for Sun workstations.
NT BugTraq www.ntbugtraq.com	Mailing list for the discussion of security exploits and security bugs in Windows NT and its related applications. Listserv available at: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM
Microsoft Security Advisory www.microsoft.com/security	Discusses security vulnerabilities in all Microsoft products and has patches available.
ANSIR advisory www.fbi.gov/hq/nsd/ansir/ansir.htm	National security threat list.
NIPC www.nipc.gov	National Infrastructure Protection Center information system advisory.
ZDNet www.zdnet.com	Product reviews and technical updates.

Resource	Contents
ISS Xforce www.iss.net	Threat analysis service.
Trend Micro Anti-Virus Support www.antivirus.com/vinfo/default.asp	Contains updated virus information including advisories and a virus encyclopedia.
Network Associates Anti-Virus Support www.nai.com	Provider of network security and availability technology.
Symantec http://securityresponse.symantec.com/	Symantec anti-virus and security advisories.
Firewalls www.isc.org/services/public/lists/firewalls.html	List for discussions of Internet firewall security systems and related issues.
INFSEC-L Information Systems Security Forum www.cert.lu/cert-web/security/News/news-infsec.txt	List for the discussion of information systems security and related issues.
Intrusion Detection Systems www.geek-girl.com/ids/about.html	<p>Forum for discussions of development of intrusion detection systems. Topics include:</p> <ul style="list-style-type: none"> • Techniques used to detect intruders in computer systems and computer networks • Audit collection/filtering • Subject profiling • Knowledge based expert systems • Fuzzy logic systems • Neural networks • Methods used by intruders (known intrusion scenarios) • CERT advisories • Scripts and tools used by hackers • Computer system policies • Universal intrusion detection system
NT Security	<p>Mailing list discussing Windows NT security as well as the Windows 95/98 and Windows for Work Group security issues. The issues discussed include everything at the host and application level security as well as at the network level.</p> <p>To subscribe, send an email message with SUBSCRIBE in the body to ntsecurity-request@iss.net.</p>