STATE OF ALABAMA

Information Technology Procedure

PROCEDURE 604P1-00: CYBER SECURITY INCIDENT REPORTING

Effective response to cyber security incidents requires quick recognition of problems, fast mobilization of skilled staff to return systems to normal, and centralized reporting.

Centralized reporting serves to increase awareness of threats, identify areas of vulnerability, allocate resources, and develop statewide solutions. Centralized reporting supports internal reporting to management, mobilizing a response team, and reporting to law enforcement, as well as supporting the postmortem analysis that is conducted after an incident.

OBJECTIVE:

Ensure effective response to cyber security incidents, protect State data from loss, and prevent disruption of government operations. These procedures implement the incident reporting and incident response assistance requirements of State IT Policy 604: Cyber Security Incident Response.

SCOPE:

These procedures apply to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

PROCEDURES:

INCIDENT IDENTIFICATION

A cyber security incident is an assessed occurrence having actual or potentially adverse effects on an information system. It's important to distinguish between problems that stem from mistakes or miscommunications and true cyber security incidents that involve either malicious intent or intent to circumvent security measures including policies, standards, and procedures. The first step in incident reporting is determining if the event is actually a cyber security incident.

In general, an incident is a violation of computer security policies, acceptable use policies, or standard computer security practices. Cyber security incidents may include, but are not limited to, the following events (regardless of platform or computing environment):

- Unauthorized access to a network, system, and/or data
- Repeated attempts at unauthorized access (from either internal or external sources)
- System changes not authorized by or known to the system owner
- Denial of Service (DoS) attack or other disruptions to service
- Evidence of tampering with, removal of, or loss of data
- Web site defacement
- Social engineering incidents
- Theft of, or non-accidental physical damage to, information systems
- Malware attacks adversely affecting servers or workstations

- Evidence of inappropriate use or other noncompliance with policies or standards
- Other incidents that could compromise the integrity of the state's information systems

Report only incidents that have a real impact (such as when damage is done, access is achieved by an attacker, loss occurs, web pages are defaced, malicious code is implanted, or policies violated) or when detecting something noteworthy or unusual (new traffic pattern, new type of malicious code, a source of persistent attacks, or evidence of inappropriate use). Do not report routine events such as periodic probes, ping sweeps, port scans, or other common events.

The following tables, derived from National Institute of Standards and Technology (NIST) Special Publication 800-61: Computer Security Incident Handling Guide, list several common malicious actions that would be considered cyber security incidents and the possible indicators of such actions. Users need to be familiar with these indicators.

Table 1: Denial of Service Indicators

Malicious Action	Possible Indicators
Network-based DoS against a particular host	• User reports of system unavailability • Unexplained connection losses • Network intrusion detection alerts • Host intrusion detection alerts (until the host is overwhelmed) • Increased network bandwidth utilization • Large number of connections to a single host • Asymmetric network traffic pattern (large amount of traffic going to the host, little traffic coming from the host) • Firewall and router log entries • Packets with unusual source addresses
Network-based DoS against a network	• User reports of system and network unavailability • Unexplained connection losses • Network intrusion detection alerts • Increased network bandwidth utilization • Asymmetric network traffic pattern (large amount of traffic entering the network, little traffic leaving the network) • Firewall and router log entries • Packets with unusual source addresses • Packets with nonexistent destination addresses
DoS against the operating system of a particular host	• User reports of system and application unavailability • Network and host intrusion detection alerts • Operating system log entries • Packets with unusual source addresses
DoS against an application on a particular host	• User reports of application unavailability • Network and host intrusion detection alerts • Application log entries • Packets with unusual source addresses

Table 2: Malicious Code Indicators

Malicious Action	Possible Indicators
A virus that spreads through e-mail infects a host.	• Antivirus software alerts of infected files • Sudden increase in the amount of e-mail being sent and received • Changes to templates for word processing documents, spreadsheets, etc. • Deleted, corrupted, or inaccessible files • Unusual items on the screen, such as odd messages and graphics • Programs start slowly, run slowly, or do not run at all • System instability and crashes • If the virus achieves root-level access, see the indicators for "Root compromise of a host" listed below under Unauthorized Access Indicators
A worm that spreads through a vulnerable service infects a host.	• Antivirus software alerts of infected files • Port scans and failed connection attempts targeted at the vulnerable service (e.g., open Windows shares, HTTP) • Increased network usage • Programs start slowly, run slowly, or do not run at all • System instability and crashes • If the worm achieves root-level access, see the indicators for "Root compromise of a host" listed below under Unauthorized Access Indicators
A Trojan horse is installed and running on a host.	• Antivirus software alerts of Trojan horse versions of files • Network intrusion detection alerts of Trojan horse client-server communications • Firewall and router log entries for Trojan horse client-server communications • Network connections between the host and unknown remote systems • Unusual and unexpected ports open • Unknown processes running • High amounts of network traffic generated by the host, particularly if directed at external host(s) • Programs start slowly, run slowly, or do not run at all • System instability and crashes • If the Trojan horse achieves root-level access, see the indicators for "Root compromise of a host" listed below under Unauthorized Access Indicators
Malicious mobile code on a Web site is used to infect a host with a virus, worm, or Trojan horse.	• Indications listed above for the pertinent type of malicious code • Unexpected dialog boxes, requesting permission to do something • Unusual graphics, such as overlapping or overlaid message boxes
Malicious mobile code on a Web site exploits vulnerabilities on a host.	• Unexpected dialog boxes, requesting permission to do something • Unusual graphics, such as overlapping or overlaid message boxes • Sudden increase in the amount of e-mail being sent and received • Network connections between the host and unknown remote systems • If the mobile code achieves root-level access, see the indicators for "Root compromise of a host" listed below under Unauthorized Access Indicators
A user receives a virus hoax message.	• Original source of the message is not an authoritative computer security group, but a government agency or an important official person • No links to outside sources • Tone and terminology attempt to invoke panic or a sense of urgency • Urges recipients to delete certain files and forward the message to others

Table 3: Unauthorized Access Indicators

Malicious Action	Possible Indicators
Root compromise of a host	• Existence of unauthorized security-related tools or exploits • Unusual traffic to and from the host (e.g., attacker may use the host to attack other systems) • System configuration changes, including: o Process/service modifications or additions o Unexpected open ports o System status changes (restarts, shutdowns) o Changes to log and audit policies and data o Network interface card set to promiscuous mode (packet sniffing) o New administrative-level user account or group • Modifications of critical files, timestamps and privileges, including executable programs, OS kernels, system libraries, and configuration and data files • Unexplained account usage (e.g., idle account in use, account in use from multiple locations at once, unexpected commands from a particular user, large number of locked-out accounts) • Significant changes in expected resource usage (e.g., CPU, network activity, full logs, or file systems) • User reports of system unavailability • Network and host intrusion detection alerts • New files or directories with unusual names (e.g., binary characters, leading spaces, leading dots) • Highly unusual operating system and application log messages • Attacker contacts the organization to say that he or she has compromised a host
Unauthorized data modification (e.g., Web server defacement, FTP warez server)	• Network and host intrusion detection alerts • Increased resource utilization • User reports of the data modification (e.g., defaced Web site) • Modifications to critical files (e.g., Web pages) • New files or directories with unusual names (e.g., binary characters, leading spaces, leading dots) • Significant changes in expected resource usage (e.g., CPU, network activity, full logs or file systems)
Unauthorized usage of standard user account	• Access attempts to critical files (e.g., password files) • Unexplained account usage (e.g., idle account in use, account in use from multiple locations at once, commands that are unexpected from a particular user, large number of locked-out accounts) • Web proxy log entries showing the download of attacker tools
Physical intruder	• User reports of network or system unavailability • System status changes (restarts, shutdowns) • Hardware is completely or partially missing (i.e., a system was opened and a particular component removed) • Unauthorized new hardware (e.g., attacker connects a packet sniffing laptop to a network or a modem to a host)
Unauthorized data access (e.g., database of customer information, password files)	• Intrusion detection alerts of attempts to gain access to the data through FTP, HTTP, and other protocols • Host-recorded access attempts to critical files

Table 4: Inappropriate Usage Indicators

Inappropriate Action	Possible Indicators
Unauthorized service usage	• Network intrusion detection and network behavior analysis software alerts • Unusual traffic to and from the host • New process/software installed and running on a host • New files or directories with unusual names • Increased resource utilization (e.g., CPU, file storage, network activity) • User reports • Application log entries (e.g., Web proxies, FTP servers, e-mail servers)
Access to inappropriate materials (e.g., downloading pornography, sending spam)	• Network intrusion detection alerts • User reports • Application log entries (e.g., Web proxies, FTP servers, e-mail servers) • Inappropriate files on workstations, servers, or removable media
Attack against external party	• Network intrusion detection alerts • Outside party reports • Network, host, and application log entries

INCIDENT RESPONSE ASSISTANCE:

Organizations that support information systems are required to provide an incident response support resource integral to the organizational incident response capability to offer information system users advice and assistance in handling and reporting security incidents.

Help Desk:

Help Desk personnel are the first line of defense for many types of incidents. Often, the first indication of an incident is a user reporting a problem to the help desk. The ISD Help Desk is the primary point of contact for all suspected cyber security incidents.

Cyber Security Incident Response Team (CSIRT):

The primary purpose of the CSIRT is to enable the State to continue critical business functions while providing rapid response to cyber security incidents. CSIRT responsibilities include incident analysis, containment, eradication, recovery, and reporting.

CSIRT Membership:

Members of the State IT Security Council and other personnel as required are subject to being called to serve on a CSIRT.

CSIRT Constituency:

IT Managers, system and network administrators, and system users state-wide.

CSIRT Authority:

For constituents that utilize ISD resources or services, the CSIRT shall have full authority to undertake any necessary actions or decisions on behalf of their constituency. For example, the CSIRT could require all affected constituents to disconnect from the network until they have installed a patch, or the CSIRT may manually intervene to disconnect those constituents that do not comply.

For constituents who control their own network segment, the State-level CSIRT acts as a coordinating team that can act alone or support agency response teams, providing direct support to the constituent and sharing in the decision-making process. For example, the CSIRT could

advise and influence constituents to disconnect from the network until a patch has been installed, or it might assist the constituency by helping with coordination and response to the advice.

Information Security Officers:

The ISD Chief Information Security Officer (CISO) normally serves as the State CSIRT Leader. Agency information security officers should lead agency response teams in coordination with the State-level CSIRT. The CSIRT Leader notifies the personnel needed to support incident response and coordinates response team communications and reporting.

Network Manager/System and Network Administrators:

System Administrators are in the best position to detect and deter cyber security incidents. Minor incidents, such as limited-impact malware infections, may be handled by the system administrator rather than activating the CSIRT.

Invite administrators and managers to review, consult, and participate in the incident response process.

Law Enforcement:

Law enforcement agencies may be able to provide assistance in cases of computer trespass, theft, threats, and other suspected criminal activities. In cases such as child pornography and other crimes against children, appropriate law enforcement agencies must be notified.

The Alabama Department of Public Safety does not have a Computer Crimes unit as such, however, the Alabama Bureau of Investigation (ABI) does have an Internet Crimes Against Children (ICAC) unit which investigates crimes of that nature (but not Internet or computer crime in general). To contact the ABI ICAC unit call 334-353-4340 weekdays 8:00am-5:00pm (Central Time) and ask for the Internet Crimes Against Children unit.

Additionally, before ABI becomes involved in any criminal investigation, the crime would have to be reported to a local law enforcement agency first and then that agency would have to request ABI assistance.

Contact local law enforcement agencies before an incident occurs to get contact information and understand the types of incidents they can assist with and what their notification requirements are. They may also be able to help with local, state, and national requirements for handling evidence. Include this information in local incident response procedures.

INCIDENT REPORTING:

Promptly report cyber security incident information to appropriate authorities in accordance with State or organization incident reporting procedures.

Initial Incident Reporting:

The single point of contact for all suspected cyber security incidents is the ISD Customer Services Center Help Desk, 334-242-2222.

When notified of a suspected cyber security incident Help Desk personnel shall immediately notify the ISD Chief Information Security Officer.

Persons reporting incidents should be prepared to provide the following information:

- Systems or sites involved
- Incident description
- Date, time, and method of incident discovery

- Category of potentially compromised data (public, internal, sensitive, or confidential)
- Actions already taken to secure or restore the system and/or data

CAUTION: Any action taken to secure or restore a system may also compromise important data that could be necessary for incident recovery and/or forensics.

On-going Communications Guidelines:

The State may suffer loss of business or reputation if public communication aspects of an incident are improperly handled, therefore, the CSIRT Leader will communicate with all parties that need to be made aware of a cyber security incident and its progress in accordance with State information dissemination policies.

It is essential that agencies establish and follow a single channel of communication. Multiple sources of information while the incident is underway creates confusion, interrupts the work of the response team, and increases vulnerability if an attacker is monitoring communications within the agency.

Determine what quantity and type of information you should communicate and whom you need to inform. Information dissemination procedures may include contacting users affected by an intrusion, security personnel, law enforcement agencies, vendors, and other business partners.

Contact managers and users affected by an incident, security personnel, law enforcement agencies, vendors, and other response teams external to the organization which may include:

United States Computer Emergency Readiness Team (US-CERT; http://www.us-cert.gov/). Reporting incidents to US-CERT is mandatory for federal agencies and for systems operating on behalf of the federal government.

Information Analysis Infrastructure Protection (IAIP). Because IAIP is part of the Department of Homeland Security (DHS), it is interested in any threats to critical U.S. infrastructures (e.g., IT and telecommunications, transportation systems, energy and utilities, agriculture, finance, healthcare, etc.). Organizations can report incidents to IAIP by contacting the National Infrastructure Coordinating Center (NICC) at nicc@dhs.gov or 202-282-9201.

CERT® Coordination Center (CERT®/CC; http://www.cert.org/). CERT®/CC is located at Carnegie Mellon University. This nongovernmental entity is interested in any computer security incidents involving the Internet.

Multi-State Information Sharing and Analysis Center (MS-ISAC). The purpose of MS-ISAC is to share important computer security-related information among its member states (which includes the state of Alabama). Several links are provided on the MS-ISAC Web site: http://www.msisac.org/.

Communicating with Law Enforcement:

If it appears a crime may have been committed, the CSIRT Leader (or an individual designated by the leader) shall coordinate with senior management and legal counsel before contacting law enforcement. Only personnel designated by management will communicate with law enforcement personnel.

Communicating with the Media:

Only the CIO (or higher authority) will address the media. The CSIRT Leader shall keep the CIO apprised of any incidents that may get or require media attention.

Protect Communications:

Share all information on a need-to-know basis and sanitize sensitive information, if required.

Be aware that communication may tip off an intruder. Communication can be overheard or picked up by an intruder so all communication relevant to an intrusion should be done in a secure manner.

Use communications that do not involve affected systems or networks such as phone and fax. Do not send e-mail over compromised systems or networks.

Communicate Upstream and Down:

Inform upstream and downstream sites of attacks and intrusions. Upstream sites are those that were involved in an intrusion prior to your system becoming involved. Downstream sites are those that were involved after your site experienced an intrusion.

In the process of analyzing an intrusion, information may be discovered about other systems that were:

- Used by an intruder to attack your systems
- Attacked by an intruder from your systems
- Used by an intruder to access your systems
- Accessed by an intruder from your systems

Such information is usually obtained from logs about connections attributed to an intruder or from remnant files left behind by an intruder. Remnant files may include scripts with the IP addresses of the attacked hosts or the output files of attack scripts an intruder neglected to delete.

Inform the administrators of all other organizations about the involvement of their systems so that they can take the necessary steps to respond to an intrusion. This includes any ISPs that may have been involved in transmitting and receiving intruder messages.

Keep accurate and detailed records of all contacts made and of the information exchanged.

Post-Incident Reporting:

Closure provides an opportunity to learn from the experience of responding to an incident. Every successful intrusion or other incident indicates potential weaknesses in systems, networks, operations, or staff preparedness. These weaknesses provide opportunities for improvement. Identify and implement lessons learned. Steps include:

- If further notification/communication is required execute this notification. Follow up with any agencies previously contacted.
- Revise security plans and procedures and conduct user and administrator training to prevent future incidents. Include any new, improved methods resulting from lessons learned.
- Determine whether or not to perform a new risk analysis based on the severity and impact of an intrusion or based on the extent of corrective action taken to restore or secure the system.
- Take a new inventory of system and network assets.
- Participate in investigation and prosecution, if applicable.

Post Mortem:

Hold a post mortem analysis and review meeting with all involved parties. Do this within three to five working days of completing the investigation of an incident.

Make a monetary estimate of the costs associated with an incident to support the business case for the level of investment in security improvement. This should include the estimated value of information assets that may have been compromised.

Develop Report:

The CISO (or CSIRT Leader) shall prepare an after-action report no later than 10 days after the incident has been certified resolved and all pertinent documentation has been received. Reports shall be presented to senior management quarterly.

ADDITIONAL INFORMATION:

Information Technology Policy 604: Cyber Security Incident Response
http://cybersecurity.alabama.gov/documents/Policy_604_Incident_Response.pdf

Information Technology Guideline 604P2: Cyber Security Incident Handling
http://cybersecurity.alabama.gov/documents/Procedure_604P2_Incident_Handling.pdf

Information Technology Dictionary
http://cybersecurity.alabama.gov/documents/IT_Dictionary.pdf

By Authority of the Office of IT Planning, Standards, and Compliance

DOCUMENT HISTORY:

Version	Release Date	Comments
600-04P1	1/12/2007	Original document
600-04P1_A	4/16/2008	Reformatted table in section 4.1. Added contact organizations to section 4.3.2. Deleted references to Form 600-04F1: Cyber Security Incident Report (form no longer used).
600-04P1_B	7/25/2008	Section 4.3.1: revised requirements for Help Desk personnel; deleted requirement to report "severity and impact of the incident."
604P1-00	6/16/2011	New number and format
604P1-00	9/24/2012	Changed the after-action report deadline from five days to ten days.