STATE OF ALABAMA

Information Technology Procedure

PROCEDURE 604P2-02: CYBER SECURITY INCIDENT HANDLING

Rapid response and collective action are required to counteract security violations and activities that lead to security breaches, and continuous improvement by applying lessons learned and eliminating points of vulnerability is essential to incident prevention. This requires prior documentation of procedures and responsibilities of everyone with a role in responding to a cyber security 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. Use these procedures as a starting point for developing the incident handling capability required for specific systems or organizational need.

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:

The incident response process as defined in NIST Special Publication 800-61 (Revision 2): *Computer Security Incident Handling Guide* has four phases:

- Preparation
- Detection and Analysis
- Containment, Eradication and Recovery
- Post-Incident Activity

The recommended and required activities of each phase are described herein.

PREPARATION

This section provides basic advice on preparing to handle incidents and on preventing incidents.

Prevention:

The following text provides a brief overview of some of the main recommended practices for preventing incidents by securing networks, systems, and applications:

Risk Assessments. Periodic risk assessments of systems and applications should determine what risks are posed by combinations of threats and vulnerabilities. Each risk should be prioritized, and the risks can be mitigated, transferred, or accepted until a reasonable overall level of risk is reached. Another benefit of conducting risk assessments regularly is that critical resources are identified, allowing staff to emphasize monitoring and response activities for those resources.

Host Security. All hosts should be hardened appropriately. In addition to keeping each host properly patched, hosts should be configured to follow the principle of least privilege. Hosts

should have auditing enabled and should log significant security-related events. The security of hosts and their configurations should be continuously monitored.

Network Security. The network perimeter should be configured to deny all activity that is not expressly permitted. This includes securing all connection points, such as virtual private networks (VPNs) and dedicated connections to other organizations.

Malware Prevention. Software to detect and stop malware should be deployed throughout the organization. Malware protection should be deployed at the host level (e.g., server and workstation operating systems), the application server level (e.g., email server, web proxies), and the application client level (e.g., email clients, instant messaging clients).

User Awareness and Training. Users should be aware of policies and procedures regarding appropriate use of networks, systems, and applications. Applicable lessons learned from previous incidents should also be shared with users so they can see how their actions could affect the organization. Improving user awareness regarding incidents should reduce the frequency of incidents. IT staff should be trained so that they can maintain their networks, systems, and applications in accordance with the organization's security standards.

Preparation:

Establish an incident response capability so that the organization is ready to respond to incidents.

The following tools and resources may be of value during incident handling:

- Contact information for team members and others within and outside the organization (primary and backup contacts), such as law enforcement and other incident response teams
- On-call information for other teams within the organization, including escalation information
- Incident reporting mechanisms, such as phone numbers, email addresses, online forms, and secure instant messaging systems that users can use to report suspected incidents
- Issue tracking system for tracking incident information, status, etc.
- Smartphones to be carried by response team members for off-hour support and on-site communications
- Encryption software to be used for communications among team members, within the organization and with external parties; software must use a FIPS-validated encryption algorithm
- War room for central communication and coordination
- Secure storage facility for securing evidence and other sensitive materials
- Digital forensic workstations and/or backup devices to create disk images, preserve log files, and save other relevant incident data
- Laptops for activities such as analyzing data, sniffing packets, and writing reports
- Spare workstations, servers, and networking equipment, or the virtualized equivalents, which may be used for many purposes, such as restoring backups and trying out malware
- Blank removable media
- Portable printer to print copies of log files and other evidence from non-networked systems
- Packet sniffers and protocol analyzers to capture and analyze network traffic
- Digital forensic software to analyze disk images
- Removable media with trusted versions of programs to be used to gather evidence from systems
- Evidence gathering accessories, including hard-bound notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape, to preserve evidence for possible legal actions

- Port lists, including commonly used ports and Trojan horse ports
- Documentation for OSs, applications, protocols, and intrusion detection and antivirus products
- Network diagrams and lists of critical assets, such as database servers
- Current baselines of expected network, system and application activity
- Cryptographic hashes of critical files to speed incident analysis, verification, and eradication
- Access to images of clean OS and application installations for restoration and recovery purposes

INCIDENT DETECTION AND ANALYSIS

Incident Categories:

Organizations should prepare generally to handle any type of incident and more specifically to handle common incident types. The incident categories listed below represent common methods of attack:

- Attrition (a denial of service or brute-force attack)
- E-mail (messages with malicious attachments or links)
- External/Removable Media (an attack executed from removable media)
- Improper Usage (violation of acceptable use policies by an authorized user)
- Loss or theft of equipment
- Web (e.g., cross-site scripting, browser hijacking)
- Other (an attack that does not fit into any of the above categories)

Incident Precursors:

Many incidents, particularly attack-type incidents, can be detected through particular precursors and indicators. Precursors and indicators are identified using many different sources, the most common being computer security software alerts, logs, publicly available information, and people.

The following table lists possible precursors to various types of incidents, and provides recommended response actions to minimize the impact of the incident or to potentially prevent a related incident from occurring.

Table 1: Incident Precursors

Precursor	Response
Unauthorized access incidents are often preceded by reconnaissance activity to map hosts and services and to identify vulnerabilities. Activity may include port scans, host scans, vulnerability scans, pings, traceroutes, DNS zone transfers, OS fingerprinting, and banner grabbing. Such activity is detected primarily through IDS software, secondarily through log analysis.	Incident handlers should look for distinct changes in reconnaissance patterns—for example, a sudden interest in a particular port number or host. If this activity points out a vulnerability that could be exploited, the organization may have time to block future attacks by mitigating the vulnerability (e.g., patching a host, disabling an unused service, modifying firewall rules).
A new exploit for gaining unauthorized access is released publicly, and it poses a significant threat to the organization.	The organization should investigate the new exploit and, if possible, alter security controls to minimize the potential impact of the exploit for the organization.

Users report possible social engineering attempts—attackers trying to trick them into revealing sensitive information, such as passwords, or encouraging them to download or run programs and file attachments.	The incident response team should send a bulletin to users with guidance on handling the social engineering attempts. The team should determine what resources the attacker was interested in and look for corresponding log-based precursors because it is likely that the social engineering is only part of the reconnaissance.
A person or system may observe a failed physical access attempt (e.g., outsider attempting to open a locked wiring closet door, unknown individual using a cancelled ID badge).	The purpose of the activity should be determined, and it should be verified that the physical and computer security controls are strong enough to block the apparent threat. (An attacker who cannot gain physical access may perform remote computing-based attacks instead.) Physical and computer security controls should be strengthened if necessary. If possible, security should detain the person. ***Note: only trained security or law enforcement personnel should attempt to detain anyone***.
An alert warns of new malicious code that targets software that the organization uses.	Research the new virus to determine whether it is real or a hoax. This can be done through antivirus vendor Web sites and virus hoax sites. If the malicious code is confirmed as authentic, ensure that antivirus software is updated with virus signatures for the new malicious code. If a virus signature is not yet available, and the threat is serious and imminent, the activity might be blocked through other means, such as configuring e-mail servers or clients to block e-mail matching characteristics of the new malicious code. The team might also want to notify antivirus vendors of the new virus.
Antivirus software detects and successfully disinfects or quarantines a newly received infected file.	Determine how the malicious code entered the system and what vulnerability or weakness it was attempting to exploit. If the malicious code might pose a significant risk to other users and hosts, mitigate the weaknesses that the malicious code used to reach the system and would have used to infect the target host.
DoS attacks are often preceded by reconnaissance activity—generally, a low volume of the traffic that will be used in the actual attack—to determine which attacks may be effective.	If handlers detect unusual activity that appears to be preparation for a DoS attack, the organization may be able to block the attack by quickly altering its security posture—for example, altering firewall rulesets to block a particular protocol from being used or protect a vulnerable host.
A newly released DoS tool could pose a significant threat to the organization.	Investigate the new tool and, if possible, alter security controls so that the tool should not be effective against the organization.

Incident Analysis:

The incident response team should work quickly to analyze and validate each incident, documenting each step taken. When the team believes that an incident has occurred, the team should rapidly perform an initial analysis to determine the incident's scope, such as which networks, systems, or applications are affected; who or what originated the incident; and how the incident is occurring (e.g., what tools or attack methods are being used, what vulnerabilities are being exploited). The initial analysis should provide enough information for the team to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident.

Detection and analysis for most types of incidents follows a very similar process; the steps, derived from NIST Special Publication 800-61: *Computer Security Incident Handling Guide*, are outlined in table 2 below.

Table 2: General Incident Handling Checklist

Detection and Analysis	
1.	Determine whether an incident has occurred
1.1	Analyze the precursors and indicators
1.2	Look for correlating information
1.3	Perform research (e.g., search engines, knowledge base)
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)
3.	Report the incident to the appropriate internal personnel and external organizations
Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence
5.	Contain the Incident
6.	Eradicate the incident
6.1	Identify and mitigate all vulnerabilities that were exploited
6.2	Remove malware, inappropriate materials, and other components
6.3	If more affected hosts are discovered, repeat the Detection & Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them
7.	Recover from the incident
7.1	Return affected systems to an operationally ready state
7.2	Confirm that the affected systems are functioning normally
7.3	If necessary, implement additional monitoring to look for future related activity
Post-Incident Activity	
8.	Create a follow-up report
9.	Hold a lessons learned meeting

INCIDENT CONTAINMENT, ERADICATION AND RECOVERY

Incident containment, eradication, and recovery steps vary based on the incident type; however, the initial containment steps are very similar. In most cases, the affected system should be isolated from the rest of the network to prevent further contamination. To preserve evidence, leave the affected system powered on. Some evidence may be lost if the system is powered off and restarted. Seek assistance as early as possible to determine the most appropriate initial incident response actions.

The remainder of this section presents containment, eradication, and recovery strategies for common incident categories.

Unauthorized Access Incidents:

Response time is critical when attempting to contain an unauthorized access incident. Extensive analysis may be required to determine exactly what has happened; and in the case of an active attack, the state of things may be changing rapidly. In most cases, it is advisable to perform an initial analysis of the incident, prioritize the incident, implement initial containment measures, and then perform further analysis to determine if the containment measures were sufficient. An appropriate combination of the following actions should be effective in the initial or final containment of an unauthorized access incident:

- Isolate the affected systems

- Disable the affected service
- Eliminate the attacker's route into the environment
- Disable user accounts that may have been used in the attack
- Enhance physical security measures

Table 3: Unauthorized Access Incident Handling Checklist

Containment, Eradication, and Recovery	
1.	Perform an initial containment of the incident
2.	Acquire, preserve, secure, and document evidence
3.	Confirm containment of the Incident
3.1	Further analyze the incident and determine if containment was sufficient
3.2	Check other systems for signs of intrusion
3.3	Implement additional containment measures if necessary
4.	Eradicate the incident
4.1	Identify and mitigate all vulnerabilities that were exploited
4.2	Remove components of the incident from systems
5.	Recover from the incident
5.1	Return affected systems to an operationally ready state
5.2	Confirm that the affected systems are functioning normally
5.3	If necessary, implement additional monitoring to look for future related activity

Malicious Code Incidents:

The checklist in Table 4 (below) provides the major steps to be performed in handling a malicious code incident. The exact sequence of steps may vary based on the nature of individual incidents and the strategies chosen by the organization for containing them.

Table 4: Malicious Code Incident Handling Checklist

Containment, Eradication, and Recovery	
1.	Acquire, preserve, secure, and document evidence
2.	Contain the incident
2.1	Identify infected systems
2.2	Disconnect infected systems from the network
2.3	Mitigate vulnerabilities that were exploited by the malicious code
2.4	If necessary, block the transmission mechanisms for the malicious code
3.	Eradicate the incident
3.1	Disinfect, quarantine, delete, and replace infected files
3.2	Mitigate the exploited vulnerabilities for other hosts within the organization
4.	Recover from the incident
4.1	Return affected systems to an operationally ready state
4.2	Confirm that the affected systems are functioning normally
4.3	If necessary, implement additional monitoring to look for future related activity

Denial of Service Incidents:

A denial of service (DoS) is an action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, or disk space. Common types of DoS attacks include reflector attacks, amplifier attacks, and floods. The exact sequence of steps may vary based on the nature of individual incidents and on the strategies chosen by the organization for halting DoS attacks that are in progress.

Table 5: Denial of Service Incident Handling Checklist

Containment, Eradication, and Recovery	
1.	Acquire, preserve, secure, and document evidence
2.	Contain the incident—halt the Denial of Service if it has not already stopped
2.1	Identify and mitigate all vulnerabilities that were used
2.2	If not yet contained, implement filtering based on the characteristics of the attack, if feasible
2.3	If not yet contained, contact the ISP for assistance in filtering the attack
2.4	If not yet contained, relocate the target
3.	Eradicate the incident: identify and mitigate all vulnerabilities that were used.
4.	Recover from the incident
4.1	Return affected systems to an operationally ready state
4.2	Confirm that the affected systems are functioning normally
4.3	If necessary and feasible, implement additional monitoring to look for future related activity

Improper Usage Incidents:

Improper usage is the use of computer or network resources in a manner that violates policies, standards, or the law. For most improper usage incidents, evidence acquisition is important. Evidence storage is also an important consideration; handling improper usage incident evidence requires discretion and confidentiality. Address the threat of having evidence altered or destroyed.

Table 6: Inappropriate Usage Incident Handling Checklist

Containment, Eradication, and Recovery	
1.	Acquire, preserve, secure, and document evidence
2.	Assess the incident
2.1	Determine whether the activity seems criminal in nature, and if necessary notify law enforcement
2.2	Discuss incident indicators and possible actions with human resources personnel
2.3	Discuss liability issues with legal counsel
2.4	Keep the investigative team small and maintain strict confidentiality
3.	If necessary, contain and eradicate the incident (e.g., remove inappropriate materials)
4.	Recover from the incident
4.1	Return affected systems to an operationally ready state
4.2	Destroy investigative materials when directed by legal counsel or law enforcement

Data Loss Incidents:

Data loss incidents may be hardware or software related, may be the result of hardware failure or destruction, software corruption, malware, human error, or theft, and may occur along with other incident types.

Table 7: Data Loss Incident Handling Checklist

Containment, Eradication, and Recovery	
1.	Acquire, preserve, secure, and document evidence
1.1	Verify authenticity and origin of data loss
1.2	Identify the data that was inappropriately disclosed, used, or lost
1.3	Identify how the data was inappropriately disclosed, used, or lost
2.	Assess the potential damage caused by data loss
2.1	Identify the individuals potentially affected by the loss of personally identifiable information (PII)
2.2	Estimate the current and potential technical effect of the incident
2.3	Estimate the potential economic damage caused by the data loss
3.	Contain the incident
3.1	Identify data distribution and protection mechanisms
3.2	Verify that data distribution and protection mechanisms are functioning properly
4.	Eradicate the incident
4.1	Review and update detection schemes and data management processes
4.2	Review and update if necessary data protection policies and standards
4.3	Regularly check previously exploited vulnerabilities and systems
5.	Recover from the incident
5.1	Restore the data from trusted backup media
5.2	Confirm that data distribution and protection mechanisms are functioning properly
5.3	Implement additional monitoring to watch for future data loss

Uncategorized Incidents:

If the incident type does not fit any particular category, follow the generic incident handling checklist (Table 2).

Multiple Component Incident Handling:

Every incident that is detected could be a multiple component incident, but it is generally better to contain the initial incident and then search for signs of other components. When an incident contains multiple component types, follow the containment, eradication, and recovery steps for each incident component and prioritize accordingly.

Evidence Gathering and Handling:

Before the analyst begins to collect any data, a decision should be made by the analyst or management (in accordance with the organization's policies and legal advisors) on the need to collect and preserve evidence in a way that supports its use in future legal or internal disciplinary proceedings. In such situations, a clearly defined chain of custody should be followed to avoid allegations of mishandling or tampering of evidence. This involves keeping a log of every person who had physical custody of the evidence, documenting the actions that they performed on the evidence and at what time, storing the evidence in a secure location when it is not being used, making a copy of the evidence and performing examination and analysis using only the copied evidence, and verifying the integrity of the original and copied evidence. If it is unclear whether or not evidence needs to be preserved, by default it generally should be preserved.

Forensics:

There are many models for the forensic process. Organizations should choose the specific forensic model that is most appropriate for their needs. Regardless of the situation, the basic forensic process is comprised of the following four phases:

Collection:

The first phase in the process is to identify, label, record, and acquire data from the possible sources of relevant data (files, operating systems, network traffic, and applications). Collection must be performed in a timely manner because of the risk of losing dynamic data, but care must be taken to preserve the integrity of the data.

Examination:

Examinations involve forensically processing large amounts of collected data using a combination of automated and manual methods to assess and extract data of particular interest, while preserving the integrity of the data. Examine copies of files, not the original files.

Analysis:

Analyze the results of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection and examination. Have a forensics toolkit for data examination and analysis.

Reporting:

The final phase is reporting the results of the analysis, which may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls), and providing recommendations for improvement to policies, procedures, tools, and other aspects of the incident response and forensic processes.

NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, provides detailed information on establishing a forensic capability. It focuses on forensic techniques for PCs, but much of the material is applicable to other systems. The document can be found at http://dx.doi.org/10.6028/NIST.SP.800-86.

POST-INCIDENT ACTIVITY

Incident Records:

Before collecting any data, a decision shall be made by management and legal counsel on the need to collect and preserve evidence in a way that supports its use in future legal or internal disciplinary proceedings. In such situations, a clearly defined chain of custody shall be followed to avoid allegations of mishandling or tampering of evidence. This involves keeping a log of every person who had physical custody of the evidence, documenting the actions they performed on the evidence and at what time, storing the evidence in a secure location when it is not being used, making a copy of the evidence and performing examination and analysis using only the copied evidence, and verifying the integrity of the original and copied evidence. If it is unclear whether or not evidence needs to be preserved, by default it generally should be preserved.

Records pertaining to cyber security incidents are confidential and shall be protected in accordance with applicable State standards.

Cyber security incident handling, reporting and follow-up records may be destroyed three years after all necessary follow-up actions have been completed unless otherwise directed by legal counsel or law enforcement personnel.

Incident Data/Metrics:

Organizations should decide what incident data to collect (for reporting/metrics purposes) based on reporting requirements and on the expected return on investment from the data (e.g., identifying a new threat and mitigating the related vulnerabilities before they can be exploited.) Focus on collecting data that is actionable.

Possible metrics for incident-related data include:

- Number of incidents handled
- Time per incident
- Objective and subjective assessments of each incident

Follow-up Report:

Create a follow-up report for each incident. The report provides a reference that can be used to assist in handling similar incidents. Include a formal chronology of events with time-stamped information such as log data from systems (important for legal reasons), Include a monetary estimate of the amount of damage the incident caused (this estimate may become the basis for subsequent prosecution activity).

Lessons Learned:

Lessons learned meetings are extremely helpful in improving security measures and the incident handling process itself. Reports from these meetings are good material for training new team members. Updating incident response policies and procedures is another important part of the lessons learned process. Post-mortem analysis of the way an incident was handled often provides impetus for change.

SUPPORTING DOCUMENTS:

- Information Technology Policy 604: Cyber Security Incident Response
- Information Technology Procedure 604P1: Cyber Security Incident Reporting

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

DOCUMENT HISTORY:

Version	Release Date	Comments
600-04P2	1/12/2007	Original document
600-04P2_A	4/16/2008	Deleted references to Form 600-04F1: Cyber Security Incident Report (form no longer used). Minor sequence changes in tables 4.1.1, 4.3.1, and 4.3.4.
604P2-00	6/16/2011	New number and format
604P2-01	09/01/2011	Format changes; tables renumbered
604P2-02	08/09/2012	Significantly revised due to changes in NIST guidance