

STATE OF ALABAMA

Information Technology Procedure

PROCEDURE 604P2-01: 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:

PREPARATION

Incident Types:

Incident handling will vary somewhat depending on the type of incident. Incident types described in these procedures include:

- Unauthorized Access
- Denial of Service (DoS)
- Malicious Code
- Inappropriate Use
- Data Loss

Incident Precursors:

Many incidents, particularly attack-type incidents, can be detected through particular precursors and indicators, primarily those listed in the following tables. These tables can easily be customized to include environment-specific precursors to facilitate a more efficient and effective incident handling process.

Table 1, Unauthorized Access Precursors, lists possible precursors to such an attack, explains the reason why each action might be performed, and provides a recommended response to potentially prevent a related incident from occurring. Additional tables of precursors for other incident types follow.

Table 1: Unauthorized Access 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.

Table 2: Malicious Code Precursors

Precursor	Response
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.

Table 3: Denial of Service Precursors

Precursor	Response
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 DETECTION AND ANALYSIS

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 4 below.

Table 4: Initial Incident Handling Checklist

Detection and Analysis	
1.	Determine whether an incident has occurred
1.1	Analyze the precursors and indicators (if applicable)
1.2	Look for correlating information
1.3	Perform research (e.g., search engines, knowledge base)
1.4	As soon as it is determined that an incident has occurred, begin documenting the investigation and gathering evidence
2.	Identify the incident type (e.g., denial of service, malicious code, unauthorized access, inappropriate usage, data loss, or multiple component)
3.	Report the incident following incident reporting procedures
4.	Prioritize handling the incident based on the business impact
4.1	Identify which resources have been affected and forecast which resources will be affected
4.2	Estimate the current and potential technical effect of the incident
5.	Follow the appropriate incident category checklist
5.1	If the incident does not fit into any of the categories, follow the generic checklist
5.2	If the incident fits more than one of the categories, follow the checklist for each category

INCIDENT CONTAINMENT, ERADICATION AND RECOVERY

Incident containment, eradication, and recovery steps vary based on the incident type. Refer to State IT Procedure 600-04P1: Cyber Security Incident Reporting for a list of incident indicators if needed to help determine the incident type.

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 5: 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 6 (below) provides the major steps to be performed in handling a malicious code incident. This checklist is a continuation of Table 4: Initial Incident Handling Checklist. Note that 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 6: 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 checklist in Table 7 (below) provides the major steps to be performed in handling a DoS incident. This checklist is a continuation of the Initial Incident Handling Checklist presented in Table 4. Note that 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 7: 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; if Step 2.1 was not performed, 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

Inappropriate Usage Incidents:

Inappropriate usage is the use of computer or network resources in a manner that violates State of Alabama policies, standards, or the law. For most inappropriate usage incidents, evidence acquisition is important. Evidence storage is also an important consideration; address the threat of having evidence altered or destroyed.

Handling inappropriate usage incidents requires discretion and confidentiality.

Table 8: 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 9: 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 checklist.

Table 10: Generic Incident Handling Checklist for Uncategorized Incidents

Containment, Eradication, and Recovery	
1.	Acquire, preserve, secure, and document evidence
2.	Contain the incident
3.	Eradicate the incident
3.1	Identify and mitigate all vulnerabilities that were exploited
3.2	Remove malicious code, inappropriate materials, and other components
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 watch for future related activity

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.

FORENSICS

The following requirements are based on the recommendations of NIST found in Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response.

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.

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.

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.

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 shall be destroyed three years after all necessary follow-up actions have been completed unless otherwise directed by legal counsel or law enforcement personnel.

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_604P1_Incident_Reporting.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
600-04P2	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