Information Security Incident Response Plan

This document describes the steps that will be taken when a cyber-intrusion incident is detected. The Office of Information Technology (OIT) will activate the Incident Response Team to engage with members of the university community as well as with appropriate outside agencies, such as law enforcement.

1) To report an information security incident, individuals are instructed to contact one of the following offices:

During regular business hours: ULM's IT Helpdesk office at 318-342-3333
Outside of normal business hours: University Police Department at 318-342-5350

2) The ULM official at the IT Helpdesk or the University Police Department will log the following information:

a) Name of the caller.
b) Time of the call.
c) Contact information about the caller.
d) The nature of the incident.
e) What equipment or persons were involved?
f) Location of equipment or persons involved.
g) How the incident was detected.
h) When the event was first noticed that supported the idea that the incident occurred.

3) The ULM official at the IT Helpdesk or the University Police Department will immediately contact the incident response manager (or designee) by phone and/or email.

4) The incident response manager (or designee) will call the designated numbers on the IT emergency contact list, in the order listed. If appropriate, the incident response manager will also contact individuals in an affected department.

5) The incident response manager (or designee) will make an initial assessment in order to answer the following questions:

a) Is the equipment affected business critical?
b) What is the severity of the potential impact?
c) Name of system being targeted, along with operating system, IP address, and location.
d) IP address and any information about the origin of the attack

6) The incident response manager (or designee) will lead the incident response team. Contacted members of the incident response team will meet or discuss the situation over the telephone/ZOOM to determine a response strategy while answering the following questions:

a) Is the incident real or perceived?
b) Is the incident still in progress?
c) What data or property is threatened and how critical is it?
d) What is the impact on the business should the attack succeed? Minimal, serious, or critical?

e) What system or systems are targeted, where are they located physically and on the network?
f) Is the incident inside the trusted network?
g) Is the response urgent?
h) Can the incident be quickly contained?
i) Will the response alert the attacker and do we care?
j) What type of incident is this? Example: virus, worm, intrusion, abuse, damage.

7) The incident response team will create an incident ticket. The incident will be categorized into the highest applicable level of one of the following categories:

a) Category one - A threat to public safety or life.
b) Category two - A threat to sensitive data
c) Category three - A threat to computer systems
d) Category four - A disruption of services

8)Team members will act according to the specific threat identified (worm response, virus response, system failure, ransomware response, etc.)

9) Team members will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Only authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary by situation and the organization.

10) Team members will restore the affected system(s) to the uninfected state. They may do any of the following:

a) Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.
b) Make users change passwords if passwords may have been compromised.
c) Ensure the system has been hardened by turning off or uninstalling unused services.
d) Ensure the system is fully patched.
e) Ensure real time virus protection and intrusion detection is running.
f) Ensure the system is logging the correct events and to the proper level.

11) Team members will document the following actions:

a) How the incident was discovered.
b) The category of the incident.
c) How the incident occurred, whether through email, firewall, etc.
d) Where the attack came from, such as IP addresses and other related information about the attacker.
e) What was the response plan.
f) What was done in response.
g) Whether the response was effective.

12) Team members will: (a) make copies of logs, email, and other communication for evidence preservation; (b) keep lists of witnesses; and (c) keep evidence as long as necessary to complete prosecution and beyond in case of an appeal. This content will be included on the IT Ticket.

13) The incident response manager (or designee) will: (a) notify the police and other appropriate external agencies, such as CISA, FBI, Attorney General of the incident; and (b) work with these agencies if prosecution of the intruder is possible.

14) Team members will assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.

15) The incident response manager (or designee) will oversee the after-action review which will focus on (a) reviewing all aspects of the incident response, (b) updating policies where necessary, and (c) taking preventative steps to minimize the risk of a similar intrusion from occurring again. The following questions will guide the review.

a) Consider whether an additional policy could have prevented the intrusion.
b) Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.
c) Was the incident response appropriate? How could it be improved?
d) Was every appropriate party informed in a timely manner?
e) Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?
f) Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
g) Have changes been made to prevent a new and similar infection?
h) Should any security policies be updated?
i) What lessons have been learned from this experience?

Team members will recommend changes to prevent the occurrence from happening again or infecting other systems. Upon management approval, the changes will be implemented.