Incident Response Procedures

Purpose

This document provides a brief overview of incident handling procedures for the UNT System Administration and Institutions. These procedures are adapted from the SANS incident handling methodology for the UNT environment. The general procedure consists of six steps: preparation, identification, containment, investigation, recovery, and follow-up. While each incident is unique, the following steps can be used as a guide.

Scope

These procedures apply to all information security incidents at the University of North Texas System Administration and Institutions.

Procedure

1. Preparation

Before incident handling takes place a number of tasks should be completed. These tasks include:
   - defining polices, standards, and procedures
   - defining the roles and responsibilities for individuals within the incident handling process
   - information gathering such as gathering contact information for individuals who are part of the process, developing system and network maps, and conducting an inventory of data
   - gathering tools and preparing job aids to facilitate a smooth incident handling process
   - reviewing and testing procedures for effectiveness

The UNT System Information Security Regulation, Information Security Handbook and the Texas Administrative Code (Chapter 202) are the policies and standards that govern incident response for UNT System institutions. The IT Shared Services Information Security Team maintains a network map, contact information for system administrators and stakeholders, and maintains a system inventory of systems that hold sensitive data or are mission critical in nature. URCM maintains an inventory of web applications and forms.

2. Identification

Identification of an incident can come from many sources. Once an incident has been identified, the person identifying the problem should:
   - contact information security to begin incident handling
   - determine the validity of the incident
   - define the scope of the incident

In addition, the IT Shared Services Information Security Team will:
   - assemble a CERT team
   - coordinate the communication amongst the CERT team
• manage the incident handling process

3. Containment

Once the incident has been validated, containment should begin immediately. The containment process includes the following steps:
• collect any live forensic data that might be relevant to the case
• inform stakeholders that the system or application will be offline
• remove the compromised system or application from public consumption
• collect relevant system forensic data
• mitigate the problem
• back up any valuable data or resources associated with the compromised system

4. Investigation

The investigative phase of the incident handling process will provide a detailed analysis of the case to determine the extent of the compromise, the nature of the problem, the steps needed to remediate the problem and prevent it from happening in the future, and the necessity to disclose the incident to the stakeholders. The investigation phase includes the following tasks:
• forensic analysis of the data collected from the compromised system
• construction of an incident report
• drafting of remediation recommendations
• reporting the incident to management

5. Recovery

The recovery phase of the incident is concerned with restoring the system or application to a working state and taking necessary actions, such as disclosure of the incident that resulted from the compromise. The following tasks occur during the recovery phase:
• repairing or rebuilding the system or application that was compromised
• restoring system data to a known good state
• validating that the problem that caused the incident has been addressed
• communicating to users that the system is back online
• disclosing the incident to effected users if necessary
• taking any appropriate administrative actions related to the incident

6. Follow-Up

The follow up phase of the incident handling process will address any remaining administrative activity related to the incident and allow us to reflect on how the experience may help us prevent similar incidents from happening in the future and adjust our procedures to make the process better. Tasks in this phase may include:
• conducting a “lessons learned” meeting with the people involved in the incident
• reporting the incident to DIR
• adjusting our policies, procedures, standards, and tools to improve the security of our systems
## Incident Handling Procedures

<table>
<thead>
<tr>
<th>Preparation</th>
<th>Identification</th>
<th>Containment</th>
<th>Investigation</th>
<th>Recovery</th>
<th>Follow Up</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Document</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communicate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Investigate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disclose</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### References

UNT System Information Security Regulation

**Contact Information**

Information Security Team  
IT Shared Services  
[http://security.unt.edu](http://security.unt.edu)  
security@unt.edu  
(940) 369-7800