

MIS Incident Report

Please return to the MIS Director.

Name: _____

Dept: _____

Phone: _____

Date: _____

PLEASE CHOOSE YOUR ANSWER BY SELECTING ONE OF THE GIVEN OPTIONS.

	Yes	No	N/A
I. Where any incidents detected during this reporting period?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

If your answer is either N/A or No, do not proceed. Submit your report to the MIS Director.

II. Incidents occurring during the reporting period.

Types of Incidents	Number of Occurrences	Descriptions/Comments
<p>1. Malicious Code Attacks. Attacks by programs typically written to masquerade presence and often difficult to detect. Include:</p> <ul style="list-style-type: none"> a. Trojan horse program b. Worms c. Scripts used to gain privileges, capture passwords, and/or modify audit logs. 	<p>_____</p> <p>_____</p> <p>_____</p>	<p>_____</p> <p>_____</p> <p>_____</p>
<p>2. Unauthorized Access. <i>Large range of incidents, including:</i></p> <ul style="list-style-type: none"> a. Unauthorized person logging into a legitimate user's account b. Unauthorized access to files and directories (by capturing super user privileges) c. A sniffer program to capture packets 	<p>_____</p> <p>_____</p> <p>_____</p>	<p>_____</p> <p>_____</p> <p>_____</p>
<p>3. Unauthorized Use. <i>Access to a user's account to perpetrate an attack is not absolutely necessary. Unauthorized use includes:</i></p>	<p>_____</p>	<p>_____</p>

- | | | |
|--|-------------------|-------------------|
| <ul style="list-style-type: none"> a. Using the network file system (NFS) to mount the file system of a remote server machine. b. Using the VMS file access listener to transfer files without authorization c. Using inter-domain access mechanisms in Windows NT to access files and directories in another organization's domain | <hr/> <hr/> <hr/> | <hr/> <hr/> <hr/> |
| <p>4. Disruption or Denial of Service.
<i>Disruptions to network and computing services. Include:</i></p> <ul style="list-style-type: none"> a. Erasing a critical program b. Spamming (flooding accounts with email) c. Altering system functionality (installing a Trojan horse) | <hr/> <hr/> <hr/> | <hr/> <hr/> <hr/> |
| <p>5. Misuse.
<i>Misuse can be intentional or unintentional include:</i></p> <ul style="list-style-type: none"> a. Use of a computing system for other than official purposes b. Changes made to system hardware, firmware, or software characteristics without the agency's knowledge, instruction, or consent. | <hr/> <hr/> | <hr/> <hr/> |
| <p>6. Hoaxes.
<i>Spreading false information about incidents or vulnerabilities. Many of these are spread via email chain letters.</i></p> | <hr/> | <hr/> |
| <p>7. Others (<i>Please describe</i>)</p> | <hr/> <hr/> | <hr/> <hr/> |

III. Incidents Profiles.

Types of Incidents	Number of Occurrences	Descriptions/Comments
1. Detected with IDS and/or log reviews	<hr/>	<hr/>
2. Unusual usage pattern	<hr/>	<hr/>
3. Caused from internal source	<hr/>	<hr/>
4. Caused from external source	<hr/>	<hr/>

Systems Affected by Incidents.

For incidents identified in section II, indicate which of the following server types were affected by entering the number of incidents per system.

Types of Servers	Number of Incidents
1. For critical production applications and/or data	_____
2. For critical administrative/support applications and/or data	_____
3. For research applications and/or data	_____
4. For academic applications and/or data	_____
5. Web servers (external use)	_____
6. Web servers (internal use)	_____
7. For FTP	_____
8. For email	_____
9. For print servers	_____
10. Other types: Identify if appropriate	_____

Additional Comments: _____

V. Response Activities and General Information.

For incidents identified in Section II, indicate from the following, the number of incidents requiring response activities.

	Number
1. How many times were incident response plans activated?	_____
2. How many times were disaster recovery plans activated due to a security incident?	_____
3. What was the average duration from detection to containment and/or restorations?	_____
4. How many reported incidents included the keeping of response activity logs?	_____
5. How many reported incidents resulted in damage to agency/university information resources assets?	_____
a. Of these how many were restored or recovered?	_____
6. How many incidents required outside assistance?	_____
7. How many incidents resulted in implementation of new security measures?	_____
a. How many were fixes, patches installed?	_____
b. How many were security software installed?	_____

- c. How many were additional policies and/or procedures developed? _____
- d. How many were other? _____
- 8. How many reported incidents resulted in proliferation (if known)? _____
 - a. Other internal systems _____
 - b. Other external systems _____
- 9. How many reported incidents resulted in external public awareness, if known? _____
- 10. Number of incidents reported to law enforcement authorities for possible prosecution? _____

Additional Comments: _____

VI. Virus Report

A. Please indicate names of the top 3 detections during reporting.

	Number of Detections	Number of Sources	
		External	Internal
1. _____	_____	_____	_____
2. _____	_____	_____	_____
3. _____	_____	_____	_____

B. For viruses identified in section A, please indicate from the following, the number of incidents which occurred.

- 1. Number of workstation hard disks infected _____
- 2. Number of floppy diskettes infected _____
- 3. Number of servers infected _____

C. Please indicate the methods of clean-up for incidents mentioned in section A.

- 1. _____
- 2. _____
- 3. _____

Additional Comments: _____

VII. Impacts

1. Total Impacts

a. What were estimated total person-hours expended on these incidents? (*mentioned in VI*)

b. What were estimated total costs as a result of the reported incidents during this reporting period

c. Any lost data unrecoverable?

Yes	No	N/A
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

d. If yes, any critical data unrecoverable?