MONTHLY INCIDENT REPORT

Agency/University Name _____

Check One: ( ) Agency ( ) University Dates covered for this reporting period: _____

Indicate Category _____

Categories.
S = Small (IR budget less than $2,000,000)
M = Medium (IR budget $2,000,000 - $10,000,000)
L = Large (IR budget greater than $10,000,000)

I. ( ) No incidents were detected during this reporting period. *(A check here completes this report.)*

II. Incidents Occurring During This Reporting Period?

(Incident types are not necessarily mutually exclusive. Report same incidents only once in the category most appropriate.)

Types of Incidents	Enter # of Occurrences	Descriptions/Comments[1]
1. Malicious Code *		
2. Unauthorized Access		
2.a. Physical Intrusion		
2.b Physical Theft		
3. Unauthorized Use		
3.a Web Site Compromises		
4. Disruption or Denial of Services (DoS)		
5. Misuse		
6. Hoaxes		
7. Others *(Please describe)*		

** This number should include virus totals listed in Section VI, Virus Report*

III. Incidents Profiles? (Responses should be numerical)

	Enter # of Incidents
1. Number detected with IDS and/or log reviews	
2. Number with unusual usage pattern	
3. Number caused from internal source	
4. Number caused from external source	

IV. Systems Affected by Incidents? (Responses should be numerical)

Type of Servers	Enter # of Incidents[1]
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	
7. other types: Identify if appropriate	

V. Response Activities and General Information[2] (Responses should be numerical)

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 restoration?	hrs.
4. How many reported incidents included the keeping of response activities logs?	
5. How many reported incidents resulted in damage to agency/university information resources assets?	
5.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?	
7.a. How many were fixes, patches installed?	
7.b. How many were security software installed?	
7.c. How many were additional policies and/or procedures developed?	
7.d. How many were other?	
8. How many reported incidents resulted in proliferation[3] (if known)?	
8.a. Other internal systems?	
8.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?[4]	

1 If an incident affects more than one type of server, report it only once in the category most appropriate.

[2] These are dependent on the types of incidents encountered? Example: Most incidents will not require activation of a disaster recovery plan.

[3] Example: Agency computer(s) used to launch attacks on other external systems?

VI. Virus Report

Names Of **Top 10** Detections During Reporting Period	# of Detections	Sources (Enter # of each type) External	Internal
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11 Number of other detections			
Total Viruses:			

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

VII. Impacts[5]

This section is crucial to the reporting process. If you do not know the exact total, please estimate.

a. What were estimated total person-hours expended on these incidents?	hrs
b. What were estimated total costs as a result of the reported incidents during this reporting period?	$
c. Any lost data unrecoverable? *(If c is YES, answer d. If NO, go to Section VIII.)*	Yes/No
d. If yes, any critical data unrecoverable?	Yes/No

Guidelines for estimating costs and person-hours

The following is intended as a guide to help assess the agency/university impacts.

a. Check to see if there are procedures and policies in place for estimating these types of impacts.

b. http://www.txdps.state.tx.us/ccrime.htm is a Department of Public Safety web site that includes formulas that can be used.

c. Consider each of the items in this list. Some, of course, may not apply.

- Downtime
- Software/hardware damage and recovery
- Time/resources used in all phases of response and recovery of systems/data/applications
- Any financial or legal liability incurred
- Theft, loss, or damage to data

---

[4] Keep in mind that anything related in any way to an incident or possible incident is potentially a piece of evidence, i.e., how the notes taken, audit logs and backups, copies of malicious code, etc. are handled

[5] Looking at costs of an incident provides data for implementation decisions on countermeasure(s) and assistance to those who may be pursuing prosecution as extra benefits.

- ☐ Reports prepared
- ☐ Investigation and pre-prosecution activity
- ☐ Major disruption of services to clients and/or mission critical functions
- ☐ Negative image/publicity

VIII. Comments to be Shared. [6]

Any practical solutions/experiences from difficulties encountered during incident response that could be of benefit to, and shared with, other agencies/universities? [7]

[6] Optional

[7] Information shared here will be shared via the IRAP email list. See www.dir.state.tx.us/IRAPC to subscribe.