XYZ College

SECURITY INCIDENT RESPONSE (*SYSTEM OWNER QUESTIONNAIRE*)

The following is a sample incident response questionnaire. The questionnaire is used by the Incident Handler to determine if the incident at the XYZ College will trigger the Critical Incident Response (CIR) procedure. The format of this report is subject to change as reporting standards and capabilities are further developed.

Assignment: Using the XYZ College Incident Response Policies, Procedures, and Framework to write 8 to 10 question that will trigger a CIR investigation.

Incident Response Handler

Question 1:	
Answer:	
Question 2:	
Answer:	
Question 3:	
Answer:	
Question 4:	
Answer:	
Question 5:	
Answer:	
Question 6:	
Answer:	
Question 7:	
Answer:	
Question 8:	
Answer:	
Question 9:	
Answer:	
Question 10:	
Answer:	

XYZ College

SECURITY INCIDENT RESPONSE *(CIR INVESTIGATION FORM)*

The following is a sample incident report. The report is an example of the types of information and incident details that will be used to track and report security incidents for XYZ College. The format of this report is subject to change as reporting standards and capabilities are further developed.

Assignment: From the information provided complete the CIR Investigation form for the incident you have been assigned.

Contact Information and Incident

Last Name: _____ First Name: _____

Job Title: _____ Cell: _____

Phone: _____ Division: _____

Mobile: _____ Department: _____

Email: _____ Office #: _____

Incident Description

Date/Time and Recovery Information

Date/Time of First Incident: Date: _____ Time: _____

Date/Time of Detected: _____ Time: _____

Has the Incident Ended? ☐ Yes ☐ No ☐ Not Known

Duration of Incident (in hours): Hours or Days

Severity of Attack: ☐ Low ☐ Medium ☐ High

Estimated Recovery Time of this Effected System (Clock) _____

Estimated Recovery Time of this Effected System (Staff Hours) _____

Number of ***Hosts*** Affected: _____

Number of ***Users*** Affected: _____

Estimated Number of Account Effected: _____

Type of Incident Detected:

☐ Exposing Confidential/Classified/ Unclassified Data	☐ Theft of Information Technology Resources/ Other Assets	☐ Creating accounts	☐ Altering DNS/Website/Data / Logs	☐ Destroying Data
☐ Anonymous FTP abuse	☐ Attacking Attackers/ Other Sites	☐ Credit Card Fraud	☐ Fraud	☐ Unauthorized Use/Access
☐ Using Machine Illegally	☐ Impersonation	☐ Increasing Notoriety of Attacker	☐ Installing a Back Door/Trojan Horse	☐ Attacking the Internet
☐ ICQ Abuse/IRC Abuse	☐ Life Threatening Activity	☐ Password Cracking	☐ Sniffer	☐ Don't Know

☐ Other (Specify) _____

CIR Response Required ☐ Yes ☐ No SB1386 - Email Notification Sent Out? ☐ Yes ☐ No

Comments (CIR Criteria):

General Information

How Did You Initially Become Aware of the Incident?

☐ Automated Software Notification	☐ Automated Review of Log Files	☐ Manual Review of Log Files	☐ System Anomaly (i. e., Crashes, Slowness)	☐ Third Party Notification
☐ Don't Know	☐ Other (Specify)			

Attack Technique (Vulnerability Exploited / Exploit Used)

☐ CVE/CERT VU or BugTraq Number	☐ Virus, Trojan Horse, Worm, or Other Malicious Code	☐ Denial of Service or Distributed Denial of Service Attack	☐ Unauthorized Access to Affected Computer Privileged Compromise (Root/Admin Access) User Account Compromise/Web Compromise (Defacement)
☐ Scanning/Probing	☐ Other		

Suspected perpetrator(s) or possible motivation(s) of attack:

☐ CSU staff/students/ faculty	☐ Former staff/ students/faculty	☐ External Party	☐ Unknown
☐ Other (Specify) _____			

XYZ College

Possible Additional Questions

Impact of Incident

Hosts

Individual Hosts

Does this Host represent an Attacking or Victim Host? ☐ Victim ☐ Attacker ☐ Both

Host Name: _____ IP Address: _____

Operating System Affected: _____ Patch Level (if known): _____

Applications Affected: _____ Database: _____

Others: _____

Primary Purpose of this Host:

☐ User Desktop Machine ☐ User Laptop Machine ☐ Web Server ☐ Mail Server ☐ FTP Server
☐ Domain Controller ☐ Domain Name Server ☐ Time Server ☐ NFS/File System Server ☐ Database Server
☐ Application Server ☐ Other Infrastructure Services

Data Compromised:

Did the incident result in a loss/compromise of sensitive or personal information? ☐ Yes (Specify) ☐ No ☐ Other

Comments:

Did the incident result in damage to system(s) or date: ☐ Yes (Specify) ☐ No ☐ Other

Comments:

Law Enforcement

Has Law Enforcement Been Notified? ☐ Yes ☐ No