Security Incident Response Plan Template
For ITS Users

January 2010

The Cyber-safety policy requires all campus units to develop, publish and maintain a security incident response plan. This security incident response plan template describes the actions that ITS Users are to follow after an incident that could represent, but is not limited to, unauthorized computer/application/data access and/or use of such systems in violation of the campus acceptable use policy. A security incident may originate from, be directed towards, or transit University controlled computer or network resources. Examples of reportable security incidents include suspected virus or worm infections and local account compromise, application or computer performance degradation, reported spam origination from a unit computer, presence of unexpected programs or files and/or unexpected application response.

The security incident response plan discussed in this document is used for initial reporting of a security incident. This plan is different from a Major Incident Report (see page 6) that reflects a formal post-incident review and analysis. It should be noted that an initial security incident report could, in fact, be later accompanied by a Major Incident Report.

Staff from each Information and Educational Technology (IET) unit has contributed to the development of the templates for incident classification and reporting. ITS has adopt these templates as our guideline.

What is a security incident?
A security incident may involve any or all of the following:

- a violation of campus computer security policies and standards,
- unauthorized computer access,
- loss of information confidentiality,
- loss of information availability,
- compromise of information integrity,
- a denial of service condition against data, network or computer,
- misuse of service, systems or information, or
- physical or logical damage to systems.

Security incident examples include but are not limited to the presence of a malicious application, such as a virus; establishment of an unauthorized account for a computer or application; unusual network connections to a computer; unusually slow computer performance; presence of unexpected/unusual programs or computer theft.

Security incident classification
All computer security incidents within ITS will be subject to classification. Security incident classification assists us to determine the severity and criticality of the security incident and ensure that the event receives the resource level attention relative to the incident priority. The classification also ensures that the security incident is reported to the appropriate manager, consistent with the priority of the security incident.

The security incident classification table, figure 1, provides several incident characteristics to assist proper incident classification. Depending on the nature of the security incident, some of the incident criteria represented in the table may not be present in a particular security breach. Moreover, if an incident contains characteristics in several different priority columns, the priority of an incident must reflect the most severe column category. For example, if a security incident affects a service that may involve personal identity information (medium priority) with a likely broad public impact (high priority), the incident should be classified as a high priority breach.

Security incident reporting
All suspected or confirmed computer security incidents within ITS will be subject to a reporting requirement. Users that identify a security incident must initially classify the incident priority based on the Security Incident Classification Table (figure 1). The initial priority level may be escalated or de-escalated by the unit desktop support staff with management approval. This initial incident priority helps to determine support staff and management engagement in a reported security incident. All incident reports are to be made within one business day after the incident was identified and with minimum delay for medium to high priority incidents.

The incident reporting table, figure 2, provides the reporting requirements for security incidents by priority level. Follow the reporting rules in figure 2.

Figure 1

Security Incident Classification Table

Incident Factors	Security Incident Report Priority Characteristics Matrix Template		
	Low	**Medium**	**High**
Criticality – Application(s) Affected	Internal Systems and Applications	Internal or External Systems and Applications	Internal or External Systems and Applications
Criticality – Infrastructure	No	Limited Scope	Campus-wide impact
Impact to User and/or System(s)	Affects few people or few systems	Department-wide impact	Campus-wide impact
Impact – Public	None	Potential Impact	Definite Impact
Countermeasures	Solutions are readily available	Weak countermeasures	No countermeasures
Resolution and/or Procedures	Available and well-defined	Resolution procedure not well-defined, bypass available	No resolution procedures or bypass available
Personally Identifiable Information	None	Possible	Definite

Minimum incident report content

Initial incident reports: Employee incident reports must include the following incident descriptors when describing the incident to unit desktop support staff:

- date and time of incident discovery
- general description of the incident
- systems and/or data at possible risk
- actions they have taken since incident discovery
- their contact information

Figure 2

Basic Security Incident Reporting Elements

Information to Record	**Description**
References	Use the assigned Remedy Help Desk Case Number or submit a case ticket
Suggested Priority Level	Low, Medium, Serious
Type of Incident	Note all types that apply: 1. Compromised System 2. Compromised User Credentials 3. Network Attacks (DOS, Scanning, Sniffing) 4. Malware (Viruses, Worms, Trojans) 5. Lost Equipment/Theft 6. Physical Break-in 7. Social Engineering (Phishing) 8. Law Enforcement Request 9. Policy Violation
Incident Timeline	Date/time that the incident was discovered Date/time that the incident was reported Date/time that the incident occurred (if known)
Who or what reported the event	Contact Information for the Incident Reporter: full name, loginUD, organizational unit/department, email address, phone number, location (mailing address, office room number). If an automated system reported the event include the name of software package, name of the host where the software is installed, physical location of the host, host or CPU ID of the host, network address of the host, and MAC address of the host if possible.
Incident Contact Information	List contact information for all parties involved in the incident.
Detailed description of the event	Include as much information as possible such as: Description of the incident (how it was detected, what occurred) Description of the affected resources Description of the affected organizations Estimated technical impact of the incident (i.e. data deleted, system crashed, application unavailable) Summary of response actions performed Other organizations contacted Cause of the incident if known (misconfigured app, unpatched host, etc.) List of evidence gathered Total hours spent on incident handling and/or additional non-labor costs involved in handling (estimate) Incident Handler Comments
Identification of the host(s)	Source of the Incident: List of sources Host name/IP Address Target of the Attack: Host Name/IP Address (note: Target of the attack should not be listed for incidents involving protected health information or sensitive student information)
Incident Handling Action Log	Include: actions taken, when, by whom
Physical Security Controls	If there is limited physical access to the computer, document the physical security controls that limit access (ask the person reporting the event to describe what they have to do to access the computer).

MAJOR INCIDENT REPORT, ITS	
Date and Time Major Incident Occurred	
Date:	Time:
Executive Summary	
Root cause: Action steps taken during incident: Remediation effort to avoid future similar incidents:	
Remedy	
List all related Remedy	
Services Impacted and Service Managers	
List all services impacted and the service manager who is involved: 1. Service, Service Manager 2. […]	
Summary Description of Major Incident	
An overview of what occurred and who was involved in the major incident.	
Summary of Major Incident Impact	
An overview of what the impact was and who, specifically, was affected (please include the types of clients impacted in a much detail as possible).	
Summary of Major Incident Outcome	
An overview of how the major incident was resolved.	
Detailed Major Incident Impact	
Additional details of the impact.	
Security Implications of Major Incident	
Details on how security was impacted or compromised.	
Detailed Major Incident Resolution	
Additional details of the steps taken to resolution. Root cause analysis.	