



# Technology Standard

## Threat Management - Incident Reporting Form

Version: 1.0

Status: Proposed: 10/30/06

Contact: [Director, Technology Services](#)

### Computer Incident Reporting Form

Use this form to report security incidents. If additional information is required, please attach a word document. Complete and submit as an attachment via [Issue Trak](#) (Issue Type: Network – Abuse) or [Abuse@vccs.edu](mailto:Abuse@vccs.edu).

<b>STATUS</b>	
<input type="checkbox"/> Site Under Attack	<input type="checkbox"/> Past Incident
<input type="checkbox"/> Repeated Incidents, unresolved	
<b>CONTACT INFORMATION</b>	
Name/Last	First: MI: Title:
Organization	
Email	
Phone:	Fax:
Location/Site(s) Involved	
Street Address Involved	
City:	State: Zip:
<b>INCIDENT DESCRIPTION</b>	
<input type="checkbox"/>	Denial of Service
<input type="checkbox"/>	Unauthorized Access (e.g. Intrusion/Hack)
<input type="checkbox"/>	Website Defacement
<input type="checkbox"/>	Malicious Code (e.g. virus/worm or trojan)
<input type="checkbox"/>	Threat/Harassment via electronic medium (includes employees)
<input type="checkbox"/>	Misuse of Systems (internal or external, includes inappropriate use by employees)
<input type="checkbox"/>	Other (specify):
<b>DATE/TIME OF INCIDENT DISCOVERY</b>	
Date	Time
Duration of Incident:	
How did you detect this?	
Has the incident been resolved? Explain.	
<b>WHO ELSE HAS BEEN NOTIFIED (Check all that apply)?</b>	
<input type="checkbox"/> System Administrator	<input type="checkbox"/> Department Director
<input type="checkbox"/> General Counsel	<input type="checkbox"/> Law Enforcement (who & when):
<input type="checkbox"/> Human Resources	<input type="checkbox"/> Other (specify)
<b>IMPACT OF INCIDENT</b>	
<input type="checkbox"/>	Loss/Compromise of Data
<input type="checkbox"/>	System Downtime
<input type="checkbox"/>	Damage to Systems

<input type="checkbox"/>	Other Organizations' Systems Affected		
<input type="checkbox"/>	Damage to the Integrity or Delivery of Critical Goods, Services or Information		
<input type="checkbox"/>	Financial Loss (estimate amount \$ )		
<b>SEVERITY OF ATTACK, INCLUDING FINANCIAL LOSS OR INFRASTRUCTURE</b>			
<input type="checkbox"/> High (e.g. defaced websites)	<input type="checkbox"/> Medium (e.g. Trojan detected)	<input type="checkbox"/> Low (e.g. Small virus outbreak)	<input type="checkbox"/> Unknown
<b>SENSITIVITY OF DATA</b>			
<input type="checkbox"/> High (e.g Privacy Act violation)	<input type="checkbox"/> Medium (e.g. local administration)	<input type="checkbox"/> Low (e.g. Public materials)	<input type="checkbox"/> Unknown
<b>IDENTIFY THE COMPUTER OPERATING SYSTEM AND ANY OTHER SOFTWARE INVOLVED</b> (Check all that apply.)			
<input type="checkbox"/> Unix	<input type="checkbox"/> OS2	<input type="checkbox"/> Linux	<input type="checkbox"/> VAX/VMS
<input type="checkbox"/> Microsoft XP/2000/NT/95/98	<input type="checkbox"/> Novell	<input type="checkbox"/> Sun OS/Solaris	
<input type="checkbox"/> Other Software (specify)			
<b>WHAT STEPS HAVE YOU TAKEN TO RESPOND</b> (Check all that apply)?			
<input type="checkbox"/> No Action Taken	<input type="checkbox"/> System disconnected from network		
<input type="checkbox"/> Restored data from backup	<input type="checkbox"/> Updated virus definitions & scanned hard drive		
<input type="checkbox"/> Physically secured computer	<input type="checkbox"/> Log files examined (saved and secured)		
<input type="checkbox"/> Other Software (specify)			

---

## RELATED LINKS

[Threat Management, Threat Detection](#)

[Threat Management, IT Security Monitoring and Logging](#)

[Threat Management, Incident Reporting](#)

---

[Return to Technology Standards](#)