

COMPUTER INCIDENT REPORTING FORM

Use this form to report security incidents to the Office of Educational Technology.

Status

Site under Attack ___ Past Incident ___ Repeated Incidents ___ Unresolved ___

Contact Information

Name/Last: _____ First: _____ MI: _____ Title: _____

Organization: _____ E-Mail: _____ Phone: _____

Location/Site(s) Involved: _____

Incident Description

___ Denial of Service Unauthorized Access (e.g., intrusion/hack)

___ Website Defacement

___ Malicious Code (e.g., virus/worm or trojan)

___ Threat/Harassment via electronic medium (includes employees)

___ Misuse of Systems (internal or external, includes inappropriate use by employees, policy violation)

___ Other, specify: _____

Date/Time of Incident Discovery

Date: _____ Time: _____

Duration of Incident: _____ How did you detect this? _____

Has the incident been resolved? Yes ___ No ___

Explain: _____

Who Else Has Been Notified (check all that apply):

___ System Administrator

___ Department Director/Data Owner

___ Human Resources

___ District Security

___ Law Enforcement (who & when: _____)

___ Other (please specify): _____

Impact of Incident

- Loss/Compromise of Data
- System Downtime
- Damage to Systems
- Other Organizations' Systems Affected
- Damage to the ___ Integrity or ___ Delivery of System Services or ___ Information

Severity of Attack, Including Financial Loss or Infrastructure

- High (defaced websites)
- Medium (trojan detected)
- Low (small virus outbreak)
- Unknown

Sensitivity of Data

- High (Privacy Act violation)
- Medium (local administration)
- Low (public materials)
- Unknown

Identify the Computer Operating System and any other Software Involved (check all that apply):

- Unix/Linux
- AS400
- Microsoft XP ___ 2000 ___ NT ___ 95/98 ___ 2003
- Other Software (specify): _____

What Steps have you Taken to Respond (check all that apply):

- No action taken system disconnected from network
- Restored data from backup, updated virus definitions and scanned hard drive
- Log files examined (saved and secured) physically secured computer
- Other (specify): _____