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): _____