



SUNY Cyber Incident Reporting Procedure

Updated 4.19.06

Summary:

University at Buffalo is required to report information security incidents to SUNY System Administration in a timely, formal way. The following types of incidents will be reported:

- Unauthorized access
- Infections by malicious code
- Denials of service
- Reconnaissance scans and probes

Incidents that are unusual and have significant impact will be reported. Malicious cyber activity that is considered normal in today's networked environment will not be reported. Examples of what to report are provided in the **Examples** section below.

The purpose of this procedure is to provide helpful information prior to and during exposure to unusual or highly damaging information security incidents. Incident reporting enables the State to provide coordination against cyber attacks and for legal actions against intruders, to facilitate warnings and share preventative information, and to collect statewide information on the frequency, impact, and cost of attacks. The overarching goal is to help all of us recover from cyber incidents in a timely and secure manner to minimize impact on other state entities.

Background:

New York State policy and SUNY System Administration require that SUNY campuses report information security incidents in a timely, formal way so that others can be warned and informed. This is an important, official duty that must be understood well by information managers and information technology staff at University at Buffalo to ensure that reports are filed efficiently and completely in all circumstances. SUNY CIOs have worked with System Administration to design a procedure that we will use and assess during the first six months of our compliance. We will begin using the procedure in February, 2005.

Scope:

This procedure applies to all information managers and information technology staff at University at Buffalo.

Responsibilities:

Information managers and information technology staff

- Responsible for notifying the **Network Operations Center** (email: noc@buffalo.edu) when an information security incident occurs.

Network Operations Center (NOC)

- Responsible for reporting information security incidents that meet the criteria described in the **Summary** section above to the SUNY System Administration (Ted Phelps, SUNY System Administration ISO). Online *Initial* and *Final Incident Report* forms are available: http://www.cscic.state.ny.us/security/incident_reporting/public_keys/incident_reporting.pdf

Associate Vice President for Information Technology

- Responsible for communicating this policy to information managers and information technology staff, maintaining, and enforcing the policy.

Procedures

When the **NOC** has determined that there is a cyber incident to report, the following procedure will be followed:

1. The System Administration Customer Services Help Desk will be called:
 - To alert the ISO and briefly describe the incident
 - To receive possible updated details on the procedures
 - If necessary, to receive a new copy of the CSCIC *Initial Report*
 - To receive instructions for password protecting the *Initial Report*
2. The completed *Initial Report* will be faxed and emailed to System Administration.
3. The final report is filed with System Administration after the incident has been understood and resolved. It reports the details of the compromised systems, source of the attack, steps taken to investigate and fix the problem and an assessment of impact on services and costs.

Examples of what to report and what not to report**Report incidents that are unusually:**

- Damaging or impending
- Threatening to life or sensitive information
- Persistent
- Wide-spread
- Resistant to defenses
- Valuable for other IT managers to know about

Type of Activity	Report/Do Not Report	Description of Activity
Access	<i>Report</i>	Access to a person's electronic HR file from unknown intruders from the Internet
	<i>Do Not Report</i>	Unauthorized reading of another person's electronic HR file by an employee who had read access but no job requirement to access it
Congestion	<i>Report</i>	A sustained denial-of-service attack on a campus resource
	<i>Do Not Report</i>	Serious network congestion caused by peer-to-peer traffic used by students
Intrusion	<i>Report</i>	Intrusion (e.g., via root) to a campus email server
	<i>Do Not Report</i>	Intrusion on a PC in a public lab
Virus Activity	<i>Report</i>	An outbreak of a new virus that is spreading rapidly
	<i>Do Not Report</i>	Normal level of virus activity, or an outbreak of a known virus in a department or college