

SCSU Security Incident Reporting Procedure

Scope

CSU Security Guidelines (document ###) requires that all Southern Connecticut State University organizations which have access to CSU systems report cyber/ computer security incidents to the SCSU Computer Incident Response Team (SCSU-CIRT). This document outlines reporting procedures to facilitate your reporting and SCSU's CIRT response activity.

SCSU's CIRT should be informed of all reportable cyber/ computer security incidents specified below. SCSU's CIRT will work with campus management to determine the severity or significance of any cyber/ computer security incident.

Reportable Cyber Security Incidents

All SCSU organizations will report cyber/ computer security related incidents that are significant or unusually persistent and meet one or more of the following criteria:

1. Unauthorized Access. All attempts at unauthorized access, whether or not they are successful, even if unauthorized access is suspected but not yet proven.
2. Malicious Code. Instances of malicious code such as viruses, Trojan horses, or worms.
3. Denial of Service. Denial of service (successful or unsuccessful) that affects or threatens to affect a critical service or denies access to all or large portions of a site's network.
4. Scans and Probes. Unauthorized network scans, probes, and attempted denial of service.

Reporting Procedures

Incidents involving unclassified computer systems

Report cyber security incidents involving unclassified systems as listed below. CIRT encourages departments to utilize the flexibility offered by e-mail whenever possible.

Non-urgent incidents

Send e-mail describing the cyber security incident to cirt@southernct.edu .
Alternatively, call the CIRT hotline at 25123, or... .

Incidents requiring immediate attention

If the cyber security incident requires priority handling, use the phrase "CIRT URGENT" in the e-mail subject line and a CIRT analyst will automatically be paged. You can also call the CIRT hotline at 25123, where an analyst will man the phone during the hours of M-F 0800-2100 EST. During off-hours, leave a voice mail with a return phone number, and a CIRT analyst will be automatically

paged and contact you immediately. **Please restrict the off-hours use of the incident hotline to only emergency situations.**

Sensitive Information

Information about unclassified cyber security incidents of a sensitive nature should be sent protected with encrypted e-mail. To facilitate this process, supply CIRT with your public encryption key, either Entrust or PGP. Contact CIRT for guidance on how to transmit information securely if encrypted means are not available.

Aggregated incident reports

Some departments find it convenient to accumulate reports and send them weekly. To facilitate the logging of these incidents, please separate the incidents into the categories listed in the previous section (Unauthorized Access, Malicious Code, Denial of Service, and Scans and Probes).

Cyber Security Incident Report Content

CIRT is available to all departments that need assistance in cyber security incident handling and gathering of incident information. In reporting cyber-related incidents to CIRT, provide as much detailed information as possible about how the incident occurred, what occurred, its impact, and what preventive measures have been implemented. Supply any log file information from the compromised system(s), routers, and/or firewalls in the communication path. CIRT will analyze this information and provide you with a detailed report regarding each unauthorized compromise.

CIRT understands that this information is not always readily available; however, any details you can provide will help with our analysis. Even if you have resolved the incident yourself, your report and analysis is valuable to CIRT in comparing this incident with those reported by other departments. It further assists CIRT in analyzing the SCSU system threat and providing management with guidance. In assessing the significance and reporting of such cyber security incidents, the reporting organization must consider the following questions:

How?

- How was access gained? What vulnerability was exploited?
- How was the incident detected?

What?

- What type of information was the compromised system processing (classified or unclassified -- OUO, UCNI, NNPI, Export Controlled)?
- What service did the system provide (DNS, key asset servers, firewall, VPN gateways, IDS)?
- What level of access did the intruder gain?
- What hacking tools and/or techniques were used?

- What did the intruder delete, modify, or steal?
- What unauthorized data collection programs, such as sniffers, were installed?
- What was the impact of the attack?
- What preventative measures have been (are being) implemented?

Who?

- Determine responsible party's identification, usually IP address(es) or host name(s).
- Does the compromise involve a country on the DOE Sensitive Country List?

When?

- When was the cyber security incident detected?
- When did the cyber security incident actually occur?

Incident Reporting Forms:

For your convenience, the Word documents listed below can be used to send CIRT the information described above.

[Compromise Incident Report Template.doc](#) - for compromised systems

[Worm Incident Report Template.doc](#) - for worm infections

[Malicious Code Incident Report Template.doc](#) - for trojans, viruses, and other non-worm malicious code incidents