



NEES IT Cybersecurity Incident Process

Version 1

March 1, 2010

NEEScomm Cybersecurity Phone Number 1-877-644-1381

Guidelines for the Cybersecurity Phone

The Cybersecurity Phone line should be used when:

- any machine used to access NEEScomm services is compromised or suspected to be compromised, including
 - Site compromise
 - Host compromise
 - Malware (flagged through anti-virus)
 - Denial of Service (flagged through anti-virus)
- any NEES account has been compromised

Cybersecurity Phone Line Process

- 1) **Receive Phone Call and Gather Information**
 - a. The Site IT Manager or equivalent person should call the cybersecurity phone number and report the incident via a voice message. The greeting message on the phone will prompt required information. The voice message will trigger a ticket which will notify the NEEScomm IT support person.
 - b. NEEScomm IT will contact the person reporting the cybersecurity incident to gather standard information, primarily IP and description of the incident. The information will be recorded in the current ticketing system and will be tagged as a cybersecurity incident.
 - c. If the Site IT Manager did not initiate the phone call, NEEScomm IT will contact the appropriate Site IT Manager and inform him/her of the situation.
 - d. After collecting information, NEEScomm IT will contact the Cybersecurity Officer and brief him on the incident. NEEScomm IT will also notify the IT Director (Dawn Weisman) and Deputy Center Director (Barb Fossum) of the incident.
- 2) **Determine if Server should be Disconnected** - Upon discussing the situation with the Cybersecurity Officer, a decision may be made for NEEScomm IT to disconnect the server in question by blocking it through IP tables.
- 3) **Evaluate Server Status** – NEEScomm IT will work with the Site IT Manager to determine if server patches are up to date and if the server has the latest anti-virus software. They will also determine what user accounts and applications have been compromised and will force a password change

- 4) **Follow up** – NEEScomm IT will meet with the Cybersecurity Officer to fully describe the server status. NEEScomm IT and the Cybersecurity Officer will determine if the server can be reconnected (via IP Tables) or if further action is needed. They will set up a conference call with the Site IT Manager to communicate findings and discuss next steps.

- 5) **Reporting** – The incident will be discussed with NEEScomm Management and Site Management to determine if the incident should be reported to NSF. All incident information will be recorded in the ticket and will be available for regular or ad-hoc reporting needs