Network Security Policy

Western Oregon University Network Security Policy

March 3, 2008

Policy:

WOU's network shall be run in a secure manner, with reasonable steps taken to protect electronic data assets owned and/or managed by Western Oregon University, and the transmission of them.

Responsibilities:

Information Services is the appropriate agency to manage and register data networks and their connection to other data networks for Western Oregon University. UCS is responsible for the design, maintenance, and operation of the overall WOU network.

Scope:

All computers connected to WOU's network must have the appropriate authorization from a recognized representative of WOU. All such authorized computers will be allowed to use an Internet Protocol (IP) address within the 140.211.0.0 class B address space owned and managed by WOU in addition to other communications protocols as appropriate. All computers connected directly to WOU's network are subject to this policy.

Actions to be taken by UCS’s systems personnel for various Network Security Events as defined later in this document:

Definitions:

CERT	Computer Emergency Response Team
DOS attack	Denial of Service Attack
NET	WOU Network Systems Team
Network	An arrangement of hardware, software, and end stations interconnected to allow sharing of electronic information.
Network Administrator	Person responsible for the network on which the affected node resides.

Port Scan Programmatically connecting to more than one TCP port and/or more than one machine.

Security event Actions taken on the network which jeopardize, or threatens to jeopardize, the integrity of WOU's Network (or other Networks) or actions which violate Federal or State Law.

SPAM Unsolicited bulk email

System Administrator Person responsible for the affected node.

1. Monitoring. NET will take reasonable steps to monitor the campus network in a way that will detect common network attacks originating either on or off campus.

2. Reporting of security Events. Security Events are to be reported to the email alias abuse@oregonstate.edu and to the node and or network administrator originating the event. Reports made by phone must be followed up with an email report. In addition to Log files showing dates, times, and specific host information regarding the event, the report must include the name and contact information for:

The person making the report.
The victim(s) of the event.
The likely perpetrators of the event.

3. Response. Once NET has determined the nature of the Event, and has an understanding of who is doing what to whom, the following actions may be taken by NET personnel:

Disable access to local hosts.
Filter remotes sites from campus network.
Both of these actions will usually be done at the campus border router in which case, email will be sent to the following aliases informing them of the block:

abuse@oregonstate.edu
support@hostname

Assuming there is no evidence that the system has been compromised, the following aliases will also be informed:

root@hostname
postmaster@hostname

In some cases, it may be appropriate to disable access to a node at a point closer to the node than the border router.

For single user workstations it may only be possible to notify the Network administrator.

Notify appropriate System Administrator and/or Network Administrators.
Notify OSU Director of Network Services.
Notify OSU campus legal authorities.
Notify law enforcement agencies.
Notify CERT.
Report incident to other sites which track specific types of abuse, ie SPAM.
Consult with local system and network administrators in securing their departmental networks.

4. Re-enabling of blocked hosts. Hosts that have had their access to the network blocked by NET will be re-enabled once NET Security personnel have a reasonable belief that the system is no longer a security risk.