Guidelines and Procedures for Blocking Network Access

Purpose:

USF must take immediate action to mitigate any threats that have the potential to pose a serious risk to the campus network, campus computers or the Internet.

If the threat is deemed serious enough, the computer(s) posing the threat will be blocked from campus network access. These guidelines specify how the decision to block is made and the procedures involved.

Data Security personnel (ISWs, ISOs and ISAs) have the obligation and authority to evaluate the seriousness and immediacy of any threat to the campus network and to take action to mitigate that threat. The action taken will be responsible and prudent based on the risk associated with that threat and the potential negative impact to the campus mission caused by making the offending computer(s) inaccessible. Examples of threats that are serious enough to invoke these procedures are:

- The level of network activity is sufficiently large as to cause serious degradation in the performance of the network;
- System administrative privileges have been acquired by someone not authorized;
- An attack on another computer or network has been launched;
- Confidential, private or proprietary electronic information or communications are being collected from the network;
- Required virus protection software is not installed and/or up to date;
- Continued complaints have been received regarding inappropriate activity and no response has been received from the departmental contact regarding the incident.

Procedures:

If the threat to the campus network or its computers is immediate, the computer(s) posing the threat will be blocked immediately and notification will be sent to the departmental security contact that the block has occurred. If the threat is not immediate, the ISO/ISA responsible for the department will be notified. If within 72 hours a response is not received indicating the department is taking action to mitigate the threat, security personnel will then block the offending computer. If a block has been put in place it will not be removed until both the department and security personnel agree that the problem causing the incident has been sufficiently addressed.

Recourse:

If a department feels that a computer has been inappropriately blocked it may request a review of the decision by the University’s Data Security Manager. An appeal of that decision can be made to the Information Security Workgroup.

Last Revision Date: 04/03/2002