

GCSU

Information Security Operational Procedures

Procedures for Blocking Network Access

PURPOSE

Georgia College & State University (GCSU) campus network and security personnel may have to take immediate action to mitigate any threats that have the potential to pose a serious risk to campus information, system resources or the Internet. If the threat is deemed a serious enough risk, the computer(s) posing the threat will be blocked from network access.

GUIDELINES

Designated GCSU campus network (CamNet) and Division of Information Technology (IT) security personnel have the authority to evaluate the seriousness and immediacy of any threat to campus information system resources or the Internet and to take action to mitigate that threat. Action that is taken will be responsible and prudent based on the risk associated with that threat and potential negative impact to the campus mission caused by making the offending computer(s) inaccessible. Example of threats that are serious enough to invoke these procedures, include but are not limited to:

- The level of network activity is sufficiently large as to cause serious degradation in the performance of the network;
- System administrative privilege have been acquired by an inappropriate individual;
- An attack on another computer or network has been launched;
- Confidential, private or proprietary information or communications are being collected;
- Continued complaints have been received regarding inappropriate activity and no response has been received from the contact regarding the incident.
- A virus, worm, or other malware has infected a computer and that computer is in turn attempting to infect other computers or networks.

PROCEDURES

If it is determined that a threat is critical, the offending computer(s) will be blocked and notification will be sent to the departmental security contact(s) via email or telephone that the block has occurred. If the threat is not immediate, notification of the threat will be sent to the departmental security contact(s) via email. If a response is not received within 4 hours indicating that the department is taking action to mitigate the threat, the offending computer(s) will be blocked. The departmental security contact(s) may request the assistance of a Technical Support Specialist in remedying the situation. In either case, campus network and security personnel will work with the departmental security contact(s) and/or the system administrator to ensure that the computer(s) are properly secured. If a block has been put in place it will be removed when both the department and IT security personnel agree that the problem causing the incident has been successfully addressed.

RECOURSE

If a department or user believes that a computer has been inappropriately blocked, either may request a review of the decision by the Chief Information Officer (CIO). If, after the review, there is still a disagreement with the decision, it will be reviewed by the CIO's superior.

Information Technology
Campus Box 050
Milledgeville, GA 31061-0490
(478) 445-1196

Revised: 03/16/09