COMPUTER VIRUS AND MALWARE POLICY

PC 11.3

POLICY STATEMENT

When a device or account connected to the GVSU campus network is compromised by a virus or malicious software, the network is at great risk of harm due to potential damage of university data or disclosure of sensitive information. To preserve the health of the network and the devices connected to it, the infected device must IMMEDIATELY be disconnected, removed and the account blocked from the campus network until Information Technology personnel verify it is no longer compromised. Despite the disruption this may cause to the individual user, the user is required to produce any infected device to Information Technology immediately upon request in order to prevent information disclosure, data file destruction, or exploitation of the compromised account.

PROCEDURES

Information Technology personnel shall provide their identification and authorization to the device user that authorizes them to remove the afflicted device prior to its removal. For additional verification, you may call the Helpdesk at 616-331-2101 and ask for Level 2 staff member to verify the authorization to pick up a computer. To minimize interruption, Information Technology will take reasonable steps to provide a substitute device for use on the campus network while the user awaits repair of the original device. To report that a device might be infected, contact Information Technology immediately at 616-331-2101.

GVSU Security Framework References

- NIST Security Framework: PR.IP-5
- Critical Security Controls (CSC): CSC 8.1