Workstation Security D 104

POLICY

1. Conditions for Use: Users may use only the IP address assigned by the Division of Information Technology or its designee.
   A. Users may not modify their assigned IP address or change/mask their MAC address to disguise their personal identity or the identity of their computer.
   B. Unless authorized by Division of Information Technology in accordance with paragraph 4 below, users may not configure their workstations to allow remote access for either authenticated or anonymous users.

2. Access Control: All workstations shall be physically secured from unauthorized access.
   A. Passwords or identifying credentials shall be sufficiently complex to reduce vulnerability and to provide for secure log-ons. See DoIT 105.
   B. Users shall not post or share their personal passwords or credentials.
   C. Users shall not use automatic log-ons or facilitate any log-on procedure that will circumvent the authentication process. Unattended workstations shall be powered off or secured in such a way as to protect the computer and network from unauthorized access.

3. Workstation Maintenance: Users shall be responsible for:
   A. Installing protection against malicious software (e.g. virus, spyware, adware, Trojan horse programs) on the workstation prior to connecting to the University network,
   B. Maintaining such software and signature files to ensure that the workstation remains protected from infection, and
   C. Ensuring that all operating system and application patches are applied.
   D. Before disposing of a workstation users shall remove all data, including all software, from the machine. Data removal must be done in such a manner that it cannot be recovered.

Users may contact the Division of Information Technology Client Support Office for instructions or assistance.

4. Workstation Remote Access: To be authorized for remote access, a workstation must be:
   A. Securely configured to allow access to only the workstation owner.
   B. Patched and updated so that there are no vulnerabilities. After review and if appropriate, the Division of Information Technology may authorize remote access.

INQUIRIES/REQUESTS:

Office of the Chief Information Officer
Room 231, Educational Communications Center
632 – 9085