Network Security D 102

SCOPE

This policy applies to all users of any University network, communication system or computer resource.

POLICY

To the fullest practical extent, the Division of Information Technology maintains an open University network while ensuring that University resources remain protected from harm that could result from cyber threat or the misuse of University facilities.

To ensure the continued integrity of its information technology systems, the University may scan any machine connected to the network and audit, inspect or monitor network usage, at any time. (See policy D 100)

1. Protection of the network – The following practices will be implemented to protect the campus network:

   A. All networks will implement appropriate security controls to protect the integrity of the data flowing over it. Additional precautions must be incorporated on network segments that contain critical information.
   B. The ISO will insure that measures are in place to mitigate any new security risks created by connecting the campus network to a 3rd party network.
   C. All connections to the campus network must be authorized by the appropriate Network Manager and reviewed by the West Campus ISO or Hospital ISO as appropriate.

2. Conditions for Access to the University Network: DoIT has established the following basic conditions for user access to the University network.

   A. Unauthorized servers are prohibited. Personal machines (not University property) which are connected to the campus network may not be used as servers.
   B. Network jacks shall be secure. Active network jacks that do not require authentication shall be physically secured or activated only when needed for use. All “public” jacks or wireless access must use authentication and encryption.
   C. Limited network connectivity. Unless a user is specifically authorized to use a different IP address by DoIT, each device connecting to the University network is limited to the IP address assigned to it.
   D. Scanning University network activity. The unauthorized installation or use of software that attempts to perform a port scan, sniff, or otherwise intercept network traffic, is strictly prohibited. Recognized departmental network administrators may perform scans for diagnostic purposes on the address space assigned to them.

3. Penetration and Intrusion Testing

   A. All computing systems that provide information through a public network, either directly or through another service that provides information externally will be subjected to penetration analysis and intrusion testing. Such analysis will be used to determine if:
      i. An individual can make an unauthorized change to an application
      ii. A user may access the application and cause it to perform unauthorized tasks.
      iii. An unauthorized individual may access the application and cause it to take actions unintended by the application designer(s)
iv. Where the campus has outsourced a server, application, or network service to another campus, penetration testing must be coordinated by both campuses.

v. Only individuals authorized by the campus ISO or delegate will perform penetration testing. The ISO and CSCIC must be notified 24 hours before penetration testing is begun. Any other attempt to perform penetration testing must be considered an unauthorized access attempt.

4. **Wireless networks**

   A. No wireless network or wireless access point will be installed without the approval of the ISO or delegate.
   B. Approved wireless networks must have suitable security, including but not limited to authentication and encryption of data traversing the wireless network.

5. **Removal from the University Network**: A machine or device may be immediately removed from the network if:

   A. The University receives a verified complaint indicating that it has been used to hack other machines or servers;
   B. A vulnerability scan reveals security issues that are not promptly corrected by the user or administrator, or
   C. investigation reveals an actual or potential misuse of University resources or the violation of state or federal law. DoIT must authorize reconnection of the machine or device to the University network after the deficiency or condition has been satisfactorily rectified.

**INQUIRIES/REQUESTS:**

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

Office of Computer Accounts  
Room112 Computing Center  
632 - 8011