NEW JERSEY CITY UNIVERSITY

Policy & Procedures

Desktop Security Guidelines

Issued by: Technology Steering Committee
Applies to: All University Employees
Effective date: June 17, 2003

In order to facilitate desktop security, the Department of Information Technology (IT) provides the following guidelines:

Activities for support personnel

- All operating system updates and patches should be applied during the setup of a computer. In addition the computer should be set up to check for and install updates automatically wherever possible.
- Updates and patches should be applied all campus-wide licensed applications installed on the computer.
- All computers should have the campus-license Enterprise McAfee anti-virus software installed and should retain the setting that schedules regular updates of virus definitions from the central server.
- New computer installation should have activated the built in firewall if available. All users should consider use of a commercial firewall, which offers additional protections not available from free products.
- Whenever possible, security policies should be set at the server level and applied to the desktop machines.
- All machines with Windows 2000 or XP should be checked with the Microsoft Baseline Security analyzer for obvious security holes.
- All compromised machines must be rebuilt by reformatting the hard drive and reinstalling all software and user data.
- When a computer is found to be compromised, ITS will disable network access from that system until it can be rebuilt or the issue corrected.

Activities for users

- Do not install "freeware" products that install spyware and other malware.
- Periodically check that OS and Anti-virus software is updating correctly.
- Develop and initiate a regular backup strategy to network storage for all university-related documents and data.
- Do not share network access login information or leave logged in computers unattended.