Computer Security

Policy 710
Date: June 20, 2006

All new computers received by the college must be processed by the office of the Director of Computing to ensure that security software and initial security settings are correct. These settings currently include the following list, but will be revised as necessary to respond to new threats to security.

The process of installing security software and making the appropriate settings includes:

1. A software firewall must be installed and working properly on all computers.
2. Current antivirus software must be installed and working on all computers.
3. All Windows computers should be set to update all Microsoft products automatically using Microsoft Update.
4. All guest accounts will be renamed and disabled.
5. All Administrator accounts will be renamed.
6. An account lockout policy should be set to 5 attempts and 30 minute lockout duration.
7. Connect computer to Hokies (for all Administrators and Staff, offer to Faculty).
8. Install security policy notice if not on Hokies.

   "By using this computer you agree to comply with Virginia Tech General Use Policies 7000 and 7010. These policies can be reviewed at http://www.policies.vt.edu."

9. Setup password protected screensavers set to activate after 15 minutes of inactivity for all computers in offices shared by more than one person.
10. Ensure that all computers require a username and password for access.
11. Ensure that initial passwords follow secure password policies.

After a user receives a secured computer it is his/her responsibility to perform any additional work necessary to stay in compliance.

Rooms that contain VT computers (including faculty offices) must be locked when not occupied.

All software applications must be legally licensed. Invoices must be available to document proof of purchase.

Change Log

Date Change:	Change By:	Summary of Change