

CSG Laptop Support Policy

This document describes the policies for service and support of laptop computers used by faculty and staff in the departments of Computer Science, Mathematics and Statistics and Actuarial Sciences running approved operating systems. The CSG (Computer Support Group), who is tasked with providing support to these three departments, will provide limited support of laptop computers. Laptop computers, due to their portability, are not typically connected to the network at all times. CSG can only provide a fully managed load to computers that remain on the network at all times, due to the way we patch and maintain software.

Definitions & Requirements

All users must adhere to the University of Iowa Acceptable Use Policies as published at <http://www.uiowa.edu/~our/opmanual/ii/19.htm>. Any activities performed on the computer that violate the University of Iowa Acceptable Use Policies may result in loss of network access.

The CSG places priority on the stability, reliability, security, and concurrency of the computer configurations and software installations. The CSG has limited resources and will support only one version of the Windows or Macintosh operating system at a time (currently Windows XP Professional and Mac OSX 10.5). Dual boot machines are not supported by CSG, though we will install software on the Windows XP or Mac OSX partition if it is already partitioned. For a system to qualify for support, it must satisfy Microsoft's or Apple's published minimum system requirements for the supported version of Windows, and either:

- a. all system hardware must be on the hardware compatibility list provided by Microsoft or Apple for the supported version of Windows/OSX, or
- b. the hardware configuration must be approved by the CSG.

When the CSG updates the version of Windows/Mac OSX it supports, all laptop computers will be reevaluated to determine eligibility for support. To maintain their support status, users may be required to upgrade their computer systems. If the system is not properly upgraded, the CSG will drop support of the system.

The laptop computer must be a University of Iowa-owned computer. Because of the portable nature of laptop computers, we cannot install software that requires a network license, e.g. Matlab, Mathematica, Scientific Workplace.

The administrative password for the laptop will be shared by CSG and by the user.

Services

The following services are provided to Windows/OSX laptop computer users:

1. CSG will install the current version of any or all of the following:
 - Microsoft Office

- UI Wireless client (Windows Only)
 - NX Client (Windows Only)
 - SecureCRT (Windows Only)
 - SSH Client (Windows Only)
 - Norton AV
 - WSFTP (Windows Only)
 - Firefox
 - Thunderbird
 - Other properly licensed software by request and as resources permit
2. CSG will configure the wireless networking for the UI Wireless network. User selection of the proper wireless card and wireless coverage is beyond the control of the CSG.
 3. CSG will configure the Windows/OSX Firewall if applicable.
 4. CSG will ensure that all software is patched to the latest version, and configure Windows/OSX to “Notify” when updates are available. Because laptops are often used with limited internet connectivity, automated patching is not practical. Security updates will be the responsibility of the user.
 5. Troubleshooting/maintenance/repair of the software installed by CSG will be limited to 30 minutes as time permits, or a full wipe/reload up to once every six months. If CSG determines that a wipe/reload is in order, we will make a good-faith effort to back up the local data.
 6. CSG will configure the Thunderbird email client.
 7. CSG will configure file and printing to the DIVMS file server and DIVMS network print queues. These services will only work when connected to the University of Iowa wired or wireless network.
 8. Warranty support. CSG will call in Dell or HP Laptops purchased with three year on-site warranty contracts. The laptop must be left with CSG for this service.

User Responsibilities

1. The user will be responsible for keeping the installation media, licensing information and driver CDs that came with the laptop. CSG will not perform any troubleshooting/maintenance/repair without the original installation media for the application in question.
2. The user will be responsible for security on the laptop.
3. Backup of local hard drives. Users are strongly urged to save all data onto the CSG file server which is backed up nightly. CSG discourages saving any data to the local hard drive. The CSG will not be able to repair or restore local files in the case of hardware failure or system problem.
4. The user will be responsible for complying with the University of Iowa data retention policy located at <http://cio.uiowa.edu/policy/policy-backup-recovery.shtml>
5. Off warranty repairs.

Best Practices

1. The user will login as a non privileged user and only login as the administrator if required. Ideally, the username of the user will match the DIVMS username to facilitate easy file transfer/drive mapping.
2. Use a hard to guess password and disable any unneeded services.
3. Use encryption software for any sensitive data.
4. For Windows users, install and run MBSA
<http://www.microsoft.com/technet/security/tools/mbsahome.mspx> to check for security updates.

See the security best practices page for more ideas
<http://cio.uiowa.edu/ITsecurity/bestprac/default.shtml>