

Baseline Security Standards

April 22, 2005

1. **UPDATES:** Keep all software (operating systems and applications) up to date to the extent possible (i.e., within compatibility and certification constraints). Configure devices to install security updates automatically, or perform the operation manually on a frequent, regular basis.
2. **ANTI-VIRUS:** Install anti-virus software on all eligible devices, using UNI site-licensed software where possible, and make certain the virus detection signatures are updated on a daily basis.
3. **ADMINISTRATOR PASSWORDS:** Configure accounts with high-level system access (e.g., administrator or root) to have long, complex passwords, and force change to them on a regular basis.
4. **SUPPORT:** Know who provides technical support for the computers you use. Those are Department IT support staff, Division IT support staff, central (ITS) support staff, or other (contracted) support staff. All names, phone numbers, and/or email addresses should be known and readily available.
5. **BACKUP:** Arrange to have/make backup copies of all important files under your control.
6. **BEST PRACTICES:** Review and implement security best practices appropriate for the device in question.