

To: All Faculty, Staff, PostDocs and Graduate Students
From: Thomas N. Jordan, Interim Department Head
Date: January 23, 2006
Subject: Department Baseline Security Policy

Computer security breaches and the proliferation of hostile software pose a real threat to data security and system integrity. The university president and provost have made it very clear that computer security is a high priority on campus and has adopted a zero tolerance policy when it comes to security breaches. If found negligent in maintaining secure practices that allowed data to be compromised, severe University and/or legal actions may be taken. It is the goal of this departmental baseline security policy to define the minimum level of security that all users must follow in order to ensure the safety of our network, data and systems.

The following policy is in effect for all departmental computer workstations and any personal systems that may acquire a Purdue network hardwired IP address:

1. A software or hardware firewall must be installed and working properly on all workstations. Botany IT will configure the firewall for all Purdue equipment.
2. Anti-virus software must be installed and working on all workstations. Virus definition files must be scheduled to update daily or automatically. Full system scans will be scheduled to occur weekly.
3. Anti-spyware software must be installed and working on all Windows workstations. Anti-spyware definition files must be set to update automatically. Currently this does not apply to Macintosh systems, but may in the future.
4. Patch management software will be installed on each workstation and set to keep the operating system and supported software patched to the latest versions. Critical patches or mitigating workarounds must be applied within 4 days of release. Non-critical OS or supported application patches must be applied within 14 days of a patch release.
5. Periodic removal of temporary files, caches, cookies and the trash folder located on the workstation's hard drive will be scheduled to occur automatically. These files are typically created by internet downloads, e-mail, e-mail attachments, installations, patches, and normal application usage.
6. A user's normal login will be assigned standard privileges with no administrative rights. A Botany IT administrative account will be created on the same workstation. Additional administrative accounts may be requested by the principle faculty/staff responsible for the workstation by completing the *Computer Security Exclusion Waiver* form. An administrative account must not be used as the user's normal login.
7. No guest accounts are allowed.

8. All accounts must be password protected using a strong password (<http://www.itap.purdue.edu/security/policies/procedures/passguidelines.cfm>). A user's password must be periodically changed according to Purdue's Authentication and Authorization Policy (http://www.purdue.edu/policies/pages/information_technology/v_1_2.html). Protect your password – do not post it in an obvious location or give it out to anyone.
9. No system shall be set to autologin.
10. A password will be required to wake a system from sleep or the screen saver at a default timing of 15 minutes of inactivity (or less). The screen should be locked or the user should log out when the workstation is unattended.
11. A user's home directory will be set to a network drive instead of the local workstation's hard drive. Default file storage locations for applications will be set to the user's designated "document" folder inside their network home directory. The network home directories will be backed up daily. It is the user's responsibility to backup any files stored on the local workstation's hard drive.
12. Server software may not be installed or activated on workstations (including, but not limited to: personal file and printer sharing, web server, e-mail server, database server, FTP server, peer-to-peer file sharing applications, etc.).
13. Users may not self-install unsupported software applications on Purdue workstations or servers unless a *Computer Security Exclusion Waiver* form is completed and approved by the department head. The requesting faculty/staff member is required to keep all unsupported software updated with the latest security patches. All shareware or purchased software must have a proof of purchase in the form of an invoice or packing slip. All freeware will require documentation that the software is free to the public or academic sector. Examples of unsupported software include but are not limited to: shareware/freeware software (games, internet downloads), instant messaging, music sharing or peer-to-peer software, personally owned software, etc.
14. Non-Purdue workstations and laptops are not permitted to plug into the Purdue ethernet PICs in order to gain access to the network. Non-Purdue systems may connect using an 802.11b/g wireless card to connect to the Purdue Airlink (PAL) wireless network and authenticate with the user's Purdue Career Account.
15. A workstation's local hard drive must never contain data that is considered to be "sensitive" or "restricted," as defined by federal and university policies (<http://www.itap.purdue.edu/security/policies/procedures/dataClassif.cfm>). All sensitive or restricted data must reside on a secure server and be documented with Botany IT. Typically, this means the following should not be stored on workstations: anyone's social security number, credit card or financial information, unencrypted passwords, or medical information. Users should continue to store non-sensitive, non-restricted documents within their home directory or network server. This also applies to Purdue systems located at home or off campus.
16. If a workstation cannot comply with any item in this baseline security policy, then a *Computer Security Exclusion Waiver* form must be completed and submitted to the department head for approval. A separate form is required for each exclusion item. <http://www.btny.purdue.edu/Pubs/SecurityExclusionWaiver.pdf>

Thank you for your cooperation as we endeavor to make our campus IT resources more secure!