END USER SECURITY GUIDELINES

Issued September 7, 2007 from the Purdue University Security Officer's Group and IT Networks and Security. Questions about these guidelines can be addressed to itap-securityhelp@purdue.edu.

I. Introduction:

Taking action to personally ensure computer security helps protect everyone from data and identity theft, viruses, hackers, and other threats. Every member of the Purdue community who uses a computing device makes Purdue’s computing environment more secure by following these guidelines.

II. Secure Computing Expectations

All end users using computing devices within Purdue’s computing environment are expected to implement the following guidelines.

End users are expected to:

- Apply computing device security software patches and updates regularly.
- Apply computing device operating system patches and updates regularly.
- Apply computing device application software patches and updates regularly (e.g. word processor software, IM clients, and other programs).
- Install and use anti-virus and anti-spyware software on the computing device, keep software definitions up to date, and run regular scans.
- Install and enable a hardware and/or software firewall.
- Use secure methods to securely transfer files (e.g., SecureFX and SecureCRT) to and from the computing device.
- Configure computing device so that it requires authentication (e.g., password, passphrase, token, or biometric authentication), runs in least privilege mode (e.g., user), and times-out after a 15 minute period of inactivity.
- Activate and utilize a lock feature prior to leaving the computing device unattended.
- Use adware removal programs regularly.
- Set the security settings to the highest level on Internet browsers and adjust downward as necessary for your Internet use.
- Regularly verify that system security measures are enabled on your computing device.
- Never share Purdue directories and files without access controls.

III. Who Should Know and Follow this Guideline?

End users are responsible for implementing this guideline on computing devices under their control which interact with Purdue’s computing environment (e.g., workstations which access Purdue IT
Resources, the Purdue Network, Purdue wireless access, Purdue ResNet, etc.). In the event that a specific computing device lacks a feature specified in this guideline, end users are expected to implement security features appropriate to the underlying computing device.

Note: Employees and other end users whose computing devices are supported by Purdue central or departmental IT units should check with their respective IT representatives prior to making changes to the security settings of those devices.

These guidelines are intended to apply to end users utilizing computing devices within Purdue’s computing environment when no other security policy, standard, or guideline applies. Nothing in this guideline shall prevent University IT Resource owners, departmental IT units, or other designated individuals from implementing guidelines or policies related to University IT Resources or computing device use within their areas of responsibility.

In keeping with these objectives, users of Purdue University IT Resources must abide by the Purdue University IT Resource Acceptable Use Policy, all other applicable Purdue University policies, and federal and state law.

The University maintains the authority to restrict or revoke any user's privileges on University IT Resources, and to take any other steps deemed necessary to manage and protect University IT Resources and data, including referral to appropriate external authorities. This authority may be exercised with or without notice to the involved users.

IV. Related References

- University IT Policies are available at:  
  http://www.purdue.edu/policies/information-technology.html

- Standards and guidelines supporting the implementation of University IT Policies are available at:  http://www.purdue.edu/securepurdue/bestPractices/

Revised November 21, 2011 to update URLs.