

Tuesday, October 21, 2008

Dear College of Education Laptop Owner,

The Education IT team has been reviewing ways to make our College computers and network as secure as possible, and ensure that we are complying with Purdue IT policies. *Education IT has identified a legacy issue related to laptops where we are out of compliance with Purdue policy.* Specifically, we have determined that several laptops in the College are using “shared” or “generic” accounts to access the laptop. Purdue policy indicates that Purdue IT resources must be accessed via a Purdue career account, and that passwords for all accounts must be changed every 30 or 120 days depending on the type of data the IT resource has access to (i.e. public, sensitive, restricted data).

We believe your area currently has at least one laptop that is using a generic account and/or automatically logs on. We need to address this issue in one of two ways:

1. Configure the laptop(s) so each person who logs into the laptop will use a Purdue career account to log on. Each user would then be responsible to change their Purdue career account password on a regular cycle. With this option, every user who logs into the laptop will *first* need to work with the IT team to add their Purdue Career Account to the laptop *before* using the laptop. **This is a good option if a small number of users will share the laptop (e.g. internal office laptop).**

2. Install a program called “DeepFreeze” on the laptop to ensure no sensitive or restricted data can be stored on the computer and that the computer cannot be compromised. DeepFreeze “resets” or “wipes” a computer to its original state each time the computer is rebooted. This resets all changes to the computer since it was last turned on. This option essentially “freezes” the computer in a clean and secure state and will allow for a generic account to be used (including allowing for auto log-on). Since no changes can be made to the computer, and since no data can be stored on the computer, there is no risk of sensitive or restricted data being compromised. The TRC uses this option for all check-out computers. **This is a good option if a large number of users will need to share the laptop (e.g. public or departmental checkout).** DeepFreeze costs approximately \$6-\$7 initially with a \$1 renewal fee each year. Ordering information for DeepFreeze can be found here:

DeepFreeze

http://research.education.purdue.edu/itodbpub/public/software_specs.asp?spec_id=222

When a computer is “Deep Frozen” data such as Word documents or PowerPoint presentations can be accessed via a removable storage device (such as a USB flash drive), or web site. While data can be temporarily stored on the local hard drive of the computer, data will be wiped when the laptop is rebooted, so it is a good idea to have a flash drive where data can be copied before powering off the laptop. Ordering information for a typical flash drive can be found here:

USB Flash Drive:

http://research.education.purdue.edu/itodbpub/public/periph_specs.asp?spec_id=841

We would like to schedule a time to work on your laptop(s) as soon as possible to make these changes. Please send email to edit@purdue.edu to let us know how you would like to proceed (option 1 or 2 above). If you have any questions, please do not hesitate to ask and we will be happy to consult with you.

The Education IT Team

edit@purdue.edu

Reference:**What is the password expiration standard for Purdue?**

<http://www.purdue.edu/securepurdue/help/view.cfm?KBTopicID=234#KB1434>

All University IT Resource passwords must be changed at least every 120 days. Faculty, staff, student-employees, and other affiliates having privileges elevated in excess of the base roles listed in the User Credentials Standard will be assigned a 30-day password expiration cycle in the OnePurdue System. In no event will a password older than 120 days be usable for access of any type to any University IT Resources.

Authentication and Authorization Policy:

http://www.purdue.edu/policies/pages/information_technology/v_1_2.html

User Credentials Standard: <http://www.purdue.edu/securepurdue/bestPractices/passStandards.cfm>

Purdue data definitions can be found here:

<http://www.itap.purdue.edu/security/policies/dataConfident/restrictions.cfm>.

Handling information for each type of data can be found here:

<http://www.itap.purdue.edu/security/procedures/dataHandling.cfm>.