PURDUE
UNIVERSITY

COLLEGE OF EDUCATION

Office of the Dean

MEMORANDUM

To: **All College of Education Faculty / Staff / Graduate Students**

From: **George W. Hynd, Dean**
Robert Evans, Director of IT

Date: **Friday, July 8, 2005**

Re: **Security Enhancements**

In response to recent security incidents at Purdue, new policies are being implemented in the College of Education related to computer security. While some of the changes may seem unpleasant, it is important to understand the severity of the problem Purdue is facing in the area of Data and IT Resource security. University IT Resources, including computer workstations have become the target of malicious attacks (increasingly by international crime syndicates), enabling perpetrators to (a) steal sensitive and restricted data to be used in Identity Theft schemes, and (b) launch attacks against servers, workstations, and IT Resources within and without Purdue. Due to the powerful and complex nature of networked computers and networked software applications, there are many ways for a workstation to be compromised, with new vulnerabilities and exploits being revealed each week.

The president and provost have made it very clear that there will be serious consequences should anyone violate security precautions and thus allow a breech similar to the ones we have recently experienced. Consequences could potentially compromise one's employment at Purdue.

The following changes are set in place to ensure that College of Education IT resources will not be accessible to unauthorized users, or for unauthorized uses.

All College of Education computer workstations must meet the following baseline security standard:

1. A firewall must be installed and working properly on all workstations
2. Current anti-virus software must be installed on all workstations
3. Server software may not be installed or activated on workstations (including, but not limited to: Microsoft File and Printer Sharing, HTTP, Email, Telnet, FTP, peer-to-peer file sharing applications). Terminal Services may be used on a workstation if additional security measures are put in place (contact Education IT for assistance).
4. Unsupported networked software applications or 3rd party software applications may not be installed or used on workstations attached to the Purdue network unless a security waiver is signed by a dean, department head, or unit director. Signed waivers will remain on file in the Education Office of Information Technology. If support for a particular software application is provided by Education IT or ITaP, software applications may be

installed and used. Requests for software installation will be processed by the Education Office of Information Technology (edit@purdue.edu). Some examples of unsupported software applications are: Shareware / Freeware Software (Games, Weather Bug, Webshots), Communications Software (Instant Messaging, Telecommunications), Peer-to-peer Software, and Music/Video Software.

5. Users may not self-install software applications on workstations attached to the Purdue network (including, but not limited to: shareware, games, communications software, peer-to-peer file sharing applications, music/video applications, and operating system enhancements). Requests for software installation will be processed by the Education Office of Information Technology (edit@purdue.edu).

Additionally, no workstation may contain local data that is considered to be "sensitive" or "restricted," as defined by University policy. All sensitive or restricted data must reside on a secure server (after consultation with Education IT). All use of sensitive or restricted data in the College of Education must be approved by a dean, department head, or unit director. Typically, this means the following should not be stored on workstations: faculty, staff, or student personal contact information, social security numbers, financial information, course rosters that contain social security numbers, DSS data or Excel spreadsheets that contain social security numbers. Users should continue to store non-sensitive, non-restricted personal documents on their local workstation.

The Education IT team has already installed firewalls and anti-virus software, on all College of Education workstations housed in BRNG. They have also removed File and Printer Sharing server software from workstations. These steps have significantly improved our IT security situation.

However, some things remain to be done.

- Users who have installed software on their College of Education workstation must remove the software or contact the Education IT team for assistance. Software to remove includes, but is not limited to: shareware, games, communications software (i.e. instant messaging), peer-to-peer file sharing applications, music/video applications, and operating system enhancements. This also applies to Purdue workstations or laptops at home.
- Those who have Purdue workstations or laptops at home should contact the Education IT team for updated firewall and/or anti-virus software.

A new initiative at Purdue called ***SecurePurdue*** is in the works and will provide security training to Purdue staff and faculty. The College of Education will also be providing in-house training to staff and faculty in coming weeks.

Purdue IT polices (including polices covering: Acceptable Use of IT Resources, Data Security, Social Security Numbers, World Wide Web, and Electronic Mail), can be found at the following address:

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

Thank you for your cooperation as we endeavor to make our College IT Resources more secure!