SECUREPURDUE NEWS
www.purdue.edu/securepurdue

July 2007
Volume 1, Issue 8

All the news that's secure to print.

Purdue updates data handling requirements

Changes strengthen and clarify rules

Purdue's Data Stewards organization recently completed changes to the University's data handling requirements, a process that began in November of 2006. The data handling requirements help Purdue faculty and staff appropriately store, transmit, and otherwise handle different types of data.

Daniel Whiteley, the student data steward, says the revisions to the requirements are to help protect the security of University data.

"The current revisions to the general requirements help to clarify some of the areas where there are frequent questions," Whiteley says. "In addition, we wanted to ensure that we are taking the best steps possible to protect our restricted and sensitive classified data. The newest revisions take additional precautions with respect to these types of data."

Revisions to the data handling requirements as a result of the review are listed below.

For handling of printed information:

- **Duplication of documents:** The restricted standard has been updated to state that the Information Owner must proactively designate material not to be further duplicated or distributed prior to distribution.
- **Mailing of documents:** The distinction in the restricted standard between campus and external mail has been eliminated. There should be no external markings on an envelope that would alert an observer or handler to the contents of the envelope.
- **Disposal of documents:** An asterisk has been added to the standard to note that use of the University confidential recycling program is acceptable for all disposal of paper documents.
- **Storage of documents:** A link in the restricted standard has been added to help illustrate what is meant by "secured location."

For handling of electronically stored (computer-based) information:

- **Storage on removable media:** A link in the restricted standard has been added to help illustrate what is meant by "secured location."
- **Print hard-copy report of information:** A link in the restricted standard has been added to help illustrate what is meant by "physical access controls." Further language encouraging immediate pickup of reports containing restricted information is added.
- **Physical destruction of media and data:**
  1) Destruction of physical electronic media that is not going to be repurposed for University use, and
  2) Destruction of data on electronic media where that media is going to be repurposed for University use.

The actual requirements have been

See DATA, Page 2

In this issue

FROM the CISO

By Scott Ksander
Executive Director
IT Networks & Security

It seems like only yesterday that I stood with excitement and anticipation in line at the computer store to be among the first to get a copy of the latest operating system: Windows 95. I couldn't wait to tear open the box and enter the next stage of the evolution of technology.

I know all engineers and technologists understand that feeling. Being "the first" to have new technology is almost as much fun as tearing open a birthday present.

Just like those birthday presents, however, we also know the sinking feeling of finding that we don't have the correct power supply or, even worse, "assembly required."

Recent releases of new, "improved," and even "more secure" software have generated a great deal of effort to move quickly to

See CISO, Page 4

SPOTLIGHT

Destroying sensitive data

In the current environment of information security, backed by the threat of legal accountability, Purdue employees often find it necessary, or even mandatory, that they utterly destroy sensitive data.

While sensitive data written on paper is easily destroyed through physical shredding, digitally-stored data can be much more difficult to eradicate.

This difficulty stems from the way computers handle and "remember" information. A computer actively "remembers" something in two primary ways. First, the computer physically writes the item into its memory, usually in the form of a magnetic storage disk, such as a hard drive. Secondly, the computer creates a pointer that "points" to the item so the computer can find it upon request.

Most of the time, when someone deletes something from their computer's memory, they drag it into a "recycling bin" or the equivalent. However, forensics experts caution that it is very difficult to truly delete information from a computer. Simply dragging a file to the Windows Recycle Bin removes the file from the screen, and may erase the computer's pointer to the file, but unless one takes additional steps to truly erase it, the sensitive files are still there, waiting for discovery by a technically savvy bad guy.

Scott Ksander, chief information security officer for Purdue, says that it is important to properly sanitize all media that contains sensitive data.

"Simply moving a file to the Recycle Bin only erases some of the computer's record of the file," Ksander says. "The information will still remain on your computer's hard disk until it is overwritten with new data. Before that data is overwritten, it is easily obtainable using standard forensic techniques, and the bad guys also have easy access to those same tools."

Short of taking a sledgehammer to the disk drive—which can actually be an effective technique—a savvy computer user does have a few less destructive options for data demolition. Today there are many disk drive "cleaning" utilities on the market. These utilities destroy all data on a drive by writing over it multiple times using both patterned and random data.

"Be sure you really want to completely wipe the entire contents of your hard drive before you use a cleaning utility. If the drive cleaned was the primary hard drive," Ksander says, "you or the new owner will have to reinstall the operating system and all programs."

Many of these utilities use standards developed by the Department of Defense and the National Institute of Standards to ensure that the data originally on the hard disk is completely destroyed. Ksander says using a cleaning utility will remove data well enough to stop recovery by anyone short of James Bond with help from "Q," and even they would find it difficult.

Once the data is removed and the computer is ready to be discarded, keep in mind that state regulations may come into play. In many states, throwing an old computer out with the garbage is prohibited. In Indiana, however, used computer monitors or televisions generated by households are considered unregulated household hazardous waste. Different regulations apply for businesses based upon the weight of the hazardous waste being discarded.

Before disposing of Purdue University assets, employees should contact their departmental IT support person, who is able to determine the best methods for disposing of departmental data.

For more information on securing a computer, including basic computer security tips, visit the SecurePurdue Web site at www.purdue.edu/SecurePurdue and review the "What should I do..." section.

DATA, from Page 1

revised to comply with the media destruction policy and refer to the media disposal guidelines.

For handling electronically-transmitted Information:

- **By fax:** A link in the restricted standard has been added to help illustrate what is meant by "physical access controls." Further language encouraging immediate pickup of reports containing restricted information is added.

Purdue's Data Stewards manage University data as a resource and an asset. As part of their responsibilities, the Data Stewards assist in the classification of data and develop handling requirements that must be followed when public, sensitive, and restricted data are handled in the course of University business.

The Data Stewards regularly review handling requirements for various types of University data, including printed information, electronically stored information, and electronically transmitted information.

For more information about the Data Stewards organization, data classification, and the data handling requirements, visit the SecurePurdue Web site at http://www.purdue.edu/securepurdue/bestPractices/dataClass.cfm

MILESTONES

ITNS staff hones skills

Increases ability to serve Purdue by adding professional tools

Six ITNS staff members recently attended SANS 401 security essentials training to gain the latest industry-current security knowledge.

The training was hosted by the SANS Institute, which stands for "SysAdmin, Audit, Network, and Security."

Doug Couch, Ben Lewis, Alan Lukens, Kitch Spicer, Cindy Welch, and Bill Harshbarger of ITNS each attended the classes, along with about 100 other Purdue staff members. Of these 100, 47 received the SANS Global Information Assurance Certification through a standardized test, and 20 more can take the test soon.

So far within ITNS, Doug, Ben, Alan, Kitch, and Bill have taken and passed the certification test.

For more information about SANS and SANS 401 training, visit the SANS Institute Web site at http://www.sans.org/.

For more information about GIAC certification, visit the GIAC Web site at http://www.giac.org/.

Purdue IT prepares for Vista

New operating system expected to arrive with students, faculty

Ready or not, Windows Vista will be coming to Purdue in August, loaded on personal computers brought by students, faculty, and staff returning to campus.

This continual advance of technology drives the need for an informed and equipped campus IT staff because, while Vista may plug existing vulnerabilities, it also provides new opportunities for novel exploits.

To prepare to embrace the new operating system, 28 Purdue IT staff will spend July 11 attending an all-day SANS video conference training session. The SANS Institute has teamed up with the University of South Carolina and Virginia Tech to deliver this pilot training opportunity for educational institutions, law enforcement agencies, and library staff. Purdue will be among 16 sites, Indiana University among them, connecting via video conference.

The session will discuss the new security-related technologies available in Windows Vista, such as "BitLocker" drive encryption, mandatory integrity control, IPSec AuthIP, the new Windows Firewall, Internet Explorer 7.0 Protected Mode, and Windows Defender, among others.

The session offers Purdue IT staff attending this training the opportunity to collaborate with IT staff from other universities who are facing similar transitional issues and concerns with the use of Vista on their networks.

For more information about security and privacy, along with the latest updates on operating systems at Purdue, visit the SecurePurdue Web site at http://www.purdue.edu/SecurePurdue.

STEAM-CIRT NEWS

STEAM-CIRT is a security and IT incident response team organized under the ITNS group within ITaP.

For more information about STEAM-CIRT and for security updates throughout the month, visit the STEAM-CIRT Web page at: http://www.purdue.edu/securepurdue/steam/

Top 10 Purdue email viruses

The following list is a 30-day snapshot of the most active email viruses on the Purdue campus.

The maximum occurrences found in one day are listed with the names of each major virus.

30-day snapshot as of July 6

Viruses	Max. Occurrences
W32/Mytob-GH	6733
W32/MyDoom-O	1339
W32/Sality-AA	638
W32/Bagle-Zip	265
W32/Mytob-Z	211
W32/Mytob-JH	197
W32/Virut-A	151
W32/Netsky-P	131
Mal/Mytob-D	105
W32/Feebs-BS	87

SECURITY RESOURCES

Use the following resources to educate yourself about security and privacy issues surrounding computers and data networks.

•IT Incident Response Report Form
http://www.purdue.edu/SecurePurdue/incidentReportForm.cfm

• Purdue data handling requirements
http://www.itap.purdue.edu/security/procedures/dataHandling.cfm

• Purdue data classification guidelines
http://www.itap.purdue.edu/security/policies/dataConfident/restrictions.cfm

• Purdue data stewards
http://www.itap.purdue.edu/ea/stewards/

• Purdue data handling roles
http://www.itap.purdue.edu/security/policies/roles.cfm

• Purdue data classifications and information owners
http://www.itap.purdue.edu/security/procedures/dataClassif.cfm

CISO, from Page 1

that new software. In addition to financial costs of making this change, new releases also bring new, and most importantly, unknown risks.

Given my background, it would seem to be heresy to suggest that we shouldn't be the earliest of early adopters. But I do want to suggest to you that, for production systems, it may not be the wisest idea to be the first on your block to expose your data to unknown risk.

Before the technical community on campus starts sending threats, virtual or otherwise, let me clearly state that I am not against aggressively investigating new technology. Testing, discovery, and learning are absolute requirements in our field.

What I ***am*** suggesting is that testing should exclude production environments and any sensitive data. By restricting new technology to isolated testing environments and using testing data that is verifiably non-sensitive, we can have all the fun we want with no fear of regrets.

Or, at least, no fear of indictment.

To realize this goal of safe testing of new technologies, we need to recognize that testing takes time. It is important that we build that time into our schedules so that organizational pressures do not force us to make choices with our production environments that are premature.

We can also benefit from the testing of others. There are many outstanding technology groups on campus, and—I'm gonna say it—"leveraging" their efforts can help everyone test new technology more quickly and with less exposure to risk.

Next time you consider bringing up the newest version of your favorite system or application on your primary office workstation or production server, remember that the best things in technology are also worth waiting for.

Thanks for reading, and, as always, be careful out there.