BALL STATE UNIVERSITY INFORMATION SECURITY

University Computing Services March 2010, Issue 1

SECURING CONFIDENTIAL INFORMATION

It's each person's responsibility at Ball State University to preserve the integrity of confidential data from the time it's received at the university until the end of it's life cycle at the university. NO one should disclose or misrepresent student or employee personal information.

Protecting confidential information is required by federal and state laws. Indiana's data protection laws require protecting Social Security Numbers, disposing of data containing confidential information and individual notification in the event of an unauthorized disclosure of electronic personal information.

This means more than just accessing personal information on your computer. It means we are to protect sensitive information in all forms. Whether it is electronic, printed or hand written we as a university and an individual can be held responsible for disclosure, or found negligent in our duty to protect it.

INDIANA DATA PROTECTION LAWS

SSN DISCLOSURE LAW

Code (IC) 4-1-10 - makes it a crime to disclose a person's Social Security Number except under certain circumstances that are spelled out in the law.

DATA DISPOSAL LAW

Code (IC) 24-4-14 - makes it a crime to dispose of certain sensitive personal information in areas accessible to the public, without taking certain steps to render it unusable by third parties.

BREACH NOTIFICATION LAW

Code (IC) 4-1-11 - requires the university to notify individuals whose personal information is reasonably exposed to unauthorized access as a result of an electronic systems security breach.

YOU, YOUR LAPTOP AND CONFIDENTIAL INFORMATION

If you have university confidential information stored on your laptop, portable computer or removable storage devices it is not only important, it is your responsibility to protect the data. University confidential information includes and not limited to student records, student financial information, credit card numbers, credit checks, bank accounts, tax records and any other confidential information maintained by the university and employees.

There is a rising number of laptop and mobile users posing security challenges for colleges and universities. Not only are they more accessible, the integrated wireless LAN capabilitie enables users to access institutional resources via third-party networks over which the institution has no direct control, and which may be attacked as a result of being attached to a public network.

On July 1, 2008 Indiana law closed a loophole in the data breach law. Prior to July 1, 2008, it was unnecessary to report an unauthorized acquisition of a portable electronic device if the device was protected by a password that had not been disclosed. As of July 1, 2008, a company does not have to report the unauthorized acquisition of a portable electronic device on which personal information is stored, if all personal information on the device is protected by encryption and the encryption key:

- has not been compromised or disclosed; and

- is not in the possession of or known to the person who, without authorization, acquired or has access to the portable electronic device.

There is no single security product or procedure that can provide complete protection, but if a laptop is password protected at power-on and uses disk encryption, device loss will not usually compromise data security.

To learn more about safeguarding confidential information on your laptop or any other portable devices contact security@bsu.edu.

FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT

The Family Educational Rights and Privacy (FERPA) Act of 1974, also referred to as the Buckley Act, is a federal law that protects the rights of student educational records.

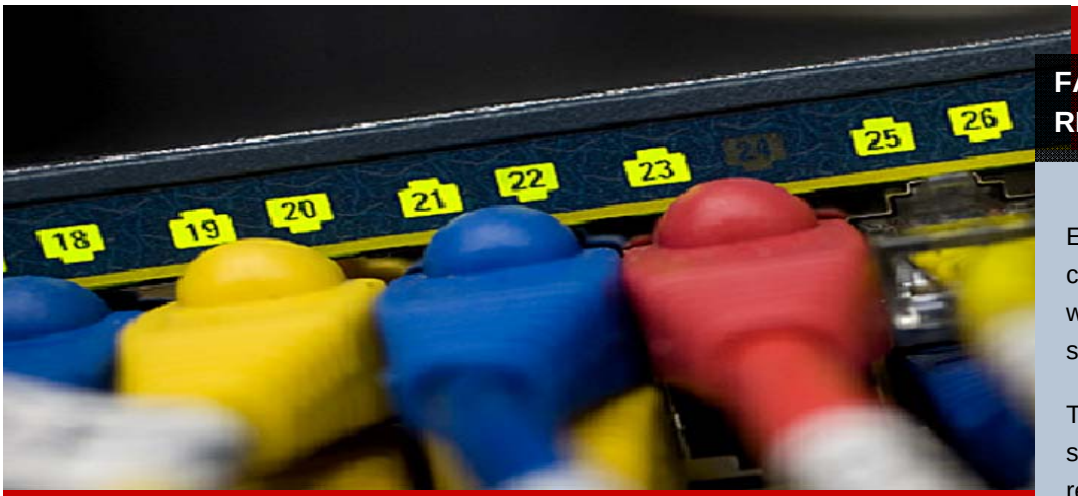
Students who are currently enrolled in school or formerly enrolled regardless of their age are subject to FERPA.

Students have a right to know about the purpose, content and location of information kept as a part of their educational records. They also have a right to expect that information in their educational records will be kept confidential unless they give permission to the school to disclose such information. Therefore, it is important to understand how educational records are defined under FERPA.

Educational records are defined by FERPA as records that directly relate to a student and that are maintained by an educational agency, an institution or by a party acting for agency or institution.

FERPA gives students the following rights regarding educational records.

- The right to access educational records kept by the school.
- The right to demand educational records be disclosed only with student consent.
- The right to amend educational records.
- The right to file complaints against the school for disclosing education records in violation of FERPA.



QUICK CHECKLIST

DO NOT use social security numbers for any purpose unless absolutely necessary. Replace them with Ball State IDs.

DO NOT link the name of a student with that student's social security number or student id in any public manner including posting of grades or printed attendance rosters.

DO NOT leave graded tests or papers in a stack for students to pick up by sorting through the tests or papers of all students.

DO NOT provide anyone with lists of students enrolled in classes for any commercial purpose.

DO NOT discuss the progress of any student without anyone other than the student (including parents/guardians) without the consent of the student.

DO NOT provide anyone with student schedules or assist anyone other than professional university employees in finding a student on campus.

Encrypt all confidential, non-directory, and sensitive personal information.

Limit the amount of personal information you give to a Web site or an individual especially if it's not required.

Shred papers containing personal/confidential information.

Use secure technology to post grades.

FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT

Educational records are considered confidential and may not be released without the written consent of the student.

There are limited exceptions when a student's consent may not be required to disclose information, including federal, state and local authorities involving an audit or evaluation of compliance with educational programs or to an accrediting organizations.

IMPORTANT POINTS FOR STUDENTS TO REMEMBER

These items are not educational records.

- Sole possession records
- Law enforcement unit records
- Employment records
- Medical records
- Alumni or post-attendance records

Information that can be released.

- Student's name
- Local/home addresses
- Local/home phone numbers
- E-mail address
- Photographs, electronic images and videos taken by the university
- Date of birth
- Dates of attendance
- Major field of study & Class Level
- Enrollment status
- Weight/height of athletic team members
- Participation in officially recognized activities and sports
- Degrees, honors and awards received
- Previous institutions

For more information on what is considered confidential under FERPA and to take a FERPA quiz visit FERPA Rights to Privacy.

PROTECT YOUR WORKPLACE

CYBER SECURITY GUIDANCE

- Update your anti-virus software daily.
- Regularly download vendor security patches for all of your software.
- Make your passwords complex. Use a combination of numbers, symbols, and letters (uppercase and lowercase).
- Change your passwords regularly, every 45 to 90 days is recommended.
- Do NOT give any of your user names, passwords or other personal access codes to anyone.
- Do NOT open e-mails or attachments from strangers.
- Do NOT install or connect any personal software or hardware without permission.
- Make electronic and physical back-ups or copies of all your most important work.
- Report all suspicious or unusual computer problems to your supervisor or to the Helpdesk.

Brought to you by the U.S. Computer Emergency Readiness Team.
Incident Hotline: 1-888-282-0870 or
www.US-CERT.gov.

OTHER LAWS THAT PROTECT YOUR PERSONAL INFORMATION

The Health Insurance Portability and Accountability Act (HIPPA) - protects the privacy of individually identifiable health information. To learn more about HIPPA visit www.hhs.gov/ocr/privacy.

Gramm-Leach-Bliley Act (GLB) - protects consumers' personal financial information held by financial institutions. To learn more about GLB visit www.ftc.gov/privacy/privacyinitiatives/glbact.

YOU ASK US

Can you spot an e-mail scam?

What is identity theft?

Let us know what you'd like to see in the next issue. Contact Security Awareness at security@bsu.edu.

BSU COMPUTER SECURITY RESPONSE TEAM

The BSU Computer Security Response Team provides an array of proactive security and incident-response services designed to protect the information assets of Ball State University. Security consulting services, proactive vulnerability assessment, intrusion detection and prevention services, security benchmarking, establishment of best-practices and procedures for information services development and deployment are examples of the services provided. Additionally, the unit promotes awareness of computer and network security related issues affecting the university through an ongoing awareness campaign. You can contact the group by e-mail at security@bsu.edu.