

MOBILE COMPUTING SECURITY POLICY

I. Purpose

The University's information is a highly important asset. The purpose of this Mobile Computing Security Policy is to protect this asset. Each employee has a responsibility to do his or her part in protecting private University information. The portability of Mobile Computing increases the possibility of compromising the integrity of our information. This policy addresses responsibilities in safeguarding this information and other issues targeted to mobile computing.

II. Individual Responsibilities

When we power up our PCs, tablets, and laptops whether from home or from our desk to access the student system, **IFAS**, **Lotus Notes**, **Blackboard**, or other university resources, we open up a window to university information. Accessing this information brings with it the responsibility of keeping that information secure. We all should minimize the chance that others will misuse our connection to this information.

Keep in mind that some of this information may reside on our tablets and laptops when we take them home, on USB flash drives, on CDs, on SmartPhones, on IPODs, on office file servers, or on other servers.

III. Protect Personal Information

There are a variety of laws that prohibit disclosing personally identifiable, non-public academic, financial or health information without permission. The Family Educational Rights and Privacy Act (FERPA) specifically targets practices of educational institutions. The Health Insurance Portability and Accountability Act (HIPAA) protects personal health-related information. These and other regulations govern the use of personal identifiers, especially the use of Social Security Numbers. The improper use of Social Security Numbers exposes individuals to identify theft, financial loss, and improper use of personal information. The Social Security Administration considers the SSN to be confidential.

The University is required to collect Social Security numbers for a number of federal purposes, and the University is allowed to use Social Security numbers for other core departmental activities which cannot be immediately facilitated by other means. However, using a spreadsheet, web site, other postings with grades, financial or medical information linked to social security numbers would violate the above laws. Personal, non-public information should not be stored on mobile devices. Whenever possible, centrally administered systems should be used to process personal non-public information. The Department of Education has ruled that using the last four digits of SSN for grade postings violates FERPA.

If you do have sensitive, non-public information (such as SSNs, grades, health information) on your portable storage media, it must be encrypted. If you transmit sensitive, non-public information over the airways or the network, it must be encrypted. Use the FHSU VPN when connecting while on the road or from home when transmitting sensitive information.

IV. Levels of Security

Accessing administrative systems from on or off campus opens university information to certain risks of exposure. Various software applications and types of connection provide access at varying levels of security. The following methods of connection and use of applications illustrate these levels.

Highly Secure:

- Connecting to a wired ethernet connection in one's office or elsewhere on campus because the connection is a switched connection (not shared).
- Using the **TigerNet** wireless SSID (mode of access) because all transmissions are encrypted.
- Using the **FHSU VPN** (virtual private network) from off-campus because this uses encryption.
- Using **QWS 3270 Secure** to access CICS (from **Jolly Giant**) because this too uses encryption. For example, entering grades with **QWS 3270 Secure** uses encryption.
- Selecting the encryption option with **Lotus Notes** (version 7 makes it easy to select encryption when sending e-mail especially to on-campus **Lotus Notes** users). Note that this works when communicating with others using **Lotus Notes** but it does not work when sending e-mail to non-**Lotus Notes** users unless special provisions are made.

Less Secure:

- Using the **TigernetStudent** wireless SSID (passwords are encrypted but transmissions are not).
- Using the **TigernetGuest** wireless SSID (the transmissions are open).
- Using **iNotes** or other web versions of **Lotus Notes** from off-campus.

V. Reporting Requirements

Should you have reason to believe that any personal information in your possession relating to any person has been, or may be intentionally or unintentionally disclosed to anyone without legitimate justification or the consent of the person to whom such information relates, you should report this circumstance as soon as possible to your immediate supervisor.

Adopted by President's Cabinet 04/04/07