PROPOSED POLICY

P02.07.066. Mobile Device Security Policy

University employees and students who use a laptop computer or mobile device (e.g. portable hard drives, USB flash drives, smartphones, tablets) are responsible for the university data stored, processed or transmitted via that computer or mobile device and for following the security requirements set forth in this policy and other applicable Information Resources Policies and regulations regardless of whether that device is the property of the university or the individual.

The use of unprotected mobile devices to access or store University non-public information as defined in R02.07.094 is prohibited regardless of whether or not such equipment is owned or managed by the university.

The Chief Information Technology Officer (CITO) is responsible for coordinating with the campuses in the development of consistent measures and business practices for ensuring the security of sensitive data on mobile devices.

PROPOSED REGULATION

R02.07.066. Mobile Device Security Policy

A. Protection of Non-Public Information

1. Every user of laptop computers or other mobile devices must use reasonable care, as outlined in the university's Information Resources Policy (P02.07), to protect university non-public information. The Information Resources Policy details examples of non-public information and the requirements for securing this data during transmission and at rest.

2. Protection of non-public information against physical theft or loss, electronic invasion, or unintentional exposure is provided through a variety of means, which include user care and a combination of technical protections, such as authentication and encryption, that work together to secure data and devices against unauthorized access.

3. The Chief Information Technology Officer (CITO) or delegate should be contacted to determine if appropriate protections are already in place and to

assist with enabling the security measures for laptops or other mobile devices. The Information Resource Policy (P02.07) details requirements for securing this data during transmission and at rest.

B. Reporting Loss/Theft of Equipment or Data

University affiliates who possess university owned laptop computers and mobile devices are expected to secure them whenever they are left unattended. The university will not reimburse for lost or stolen, personally owned laptop computer(s) or other mobile device(s).

In the event a university-owned or managed laptop computer or mobile device is lost or stolen, the following steps should be taken:

1. Immediately report the theft or loss to the respective campus support center/helpdesk who will:
   - 1.1. Immediately report the theft or loss to the respective campus University Police Department or local law enforcement.
   - 1.2. Contact the Office of Information Technology to report the incident which will initiate a risk assessment by the Chief Information Security Officer.
   - 1.3. Contact your Risk Management Office to file a stolen property claim.

In the event university non-public information is contained on any mobile device that is lost or stolen, or if passwords or other system access control mechanisms are lost, stolen or disclosed, or are suspected of being lost, stolen or disclosed the Chief Information Security Officer must be contacted immediately.

C. Use of Personal Mobile Devices

The use of personal laptops and other mobile devices to conduct University business is not encouraged, however incidental use of personal equipment shall comply with all policies and regulation regarding use of Mobile Devices.

Employees acknowledge a personally owned laptop computer or mobile device used to access, store or transmit university data or resources is subject to sequestration for forensic examination by the University in the event a device is involved in legal processes, has been compromised or otherwise may have have exposed non-public university data.

D. Securing Information on Mobile Devices

The CITO will coordinate the establishment of appropriate guidelines for securing mobile devices and will promulgate these as technology changes.

E. Devices that do not support encryption must not be used to access, store, or manipulate restricted information.

F. In addition to appropriate information handling requirements determined by the Information Resources data classification, sector-specific data (ex. PCI-DSS, HIPAA, etc.) may have additional requirements. Check with the Office of Information Technology for assistance.

G. Individual divisions, schools, colleges, Institutes or departments may impose additional information security requirements beyond those set forth in this policy and as may be required by sponsors, government agencies or other external entities. For further information on reporting security incidents and implementing security practices see the Office of Information Technology website.

H. Requirements When Traveling Overseas

University personnel and students carrying university-issued laptops or mobile devices while traveling abroad, whether on business or for pleasure, must comply with data protection measures in this policy and with U.S. trade control laws, the university's regulation on Export Control Licensing and laws of the destination country. U.S. export control laws may prohibit or restrict such activities absent special U.S. government licenses. Before traveling abroad with a laptop or other mobile device, consult with the Office of Information Technology, your funding agency, Office of Research Integrity (ORI) or Vice-Chancellor of Research.

University faculty, staff, and students must understand the restrictions described here, which may include prohibiting the use of any device(s) that may later come in contact with any UA network..