INFORMATION TECHNOLOGY
UNIVERSITY of WASHINGTON | TACOMA

POLICY TITLE: Data Protection Policy for Portable Devices

Rationale

According to Washington State Law RCW 42.17.31922 (http://apps.leg.wa.gov/RCW/default.aspx?cite=42.17.31922), any State and local agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The following policy addresses compliance issues related to the above State Law.

Scope

This policy only addresses encrypting data stored on a portable device, such that if the device is lost or stolen, the data are essentially useless to unauthorized users. It does not address the transmission of unencrypted data across a network, including reading or storing data from your desktop or portable device to/ from the network storage area.

The Policy

Every UWT employee is expected to store confidential data, human subjects data or personally identifiable information as specified by Washington State Law RCW 42.17.31922, in the UWT network storage areas provided by Computer Services. Every UWT employee has a network home directory and departmental storage area.

If any UWT employee must move or copy confidential data, human subjects data or personally identifiable information as specified by Washington State Law RCW 42.17.31922, to portable devices from UWT network server areas, the person has to provide encryption to protect the data stored on the portable device. The employee is expected to contact Computer Services before placing confidential data, human subjects data or any other personally identifiable information onto any portable device. If necessary, Computer services will install, configure and train the employee on the use of the encryption software. Portable devices include but are not limited to: laptops, USB storage devices (e.g. thumb/ jump drives), external hard drives, PDAs, removable media including flash memories (e.g. Compact Flash, Memory Stick, Secure Digital), floppy disks, CD-RWs and zip disks. (Note: Not all portable devices are capable of storing encrypted data; Computer Services will review with the users as required).

For more information, please also refer to the UW Electronic Information Privacy Policy on Personally Identifiable Information web page. http://www.washington.edu/computing/rules/privacypolicy.htm