Personally Owned Devices and User Responsibility with SPG 601.33

Implementation by end of CY2014

Prepared by Ron Loveless
IT Manager, Plant Operations
June 16, 2014
What is SPG 601.33?

Security of Personally Owned Devices That Access or Maintain Sensitive Institutional Data:

• Acknowledges that the university may permit employees to work with sensitive institutional data on personally owned devices
• Directs members of the University community who work with sensitive institutional data on personally owned devices to properly self-manage the privacy and security settings on their device

• Plant Operations is adopting SPG 601.33 as its official policy with no additional unit level restrictions
• Implementation expected by end of CY 2014, December 31, 2014
• The Good News: Does not apply to the majority of Plant staff!
What is a Personally Owned Device (POD)?

Any computing device that you own that is used for UM business:

• Personal PC
• Smartphone
• Personal Laptop
• Tablet (iPad, Slate, MS Surface)
• Google Glass
• Etc...
What is Sensitive Institutional Data?

Sensitive Institutional Data is data whose unauthorized disclosure may have serious adverse effect on the University’s reputation, resources, services, or individuals. Data protected under federal or state regulations or due to proprietary, ethical, or privacy considerations will typically be classified as sensitive (SPG 601.12)

Examples include:

- Social Security Numbers
- Student Educational Records
- Patient Health/Medical Information
- Certain types of information about hazardous substances
- Certain types of blueprints and building plans
Your Responsibilities

• Self-manage and secure your POD by following the minimum device management and security expectations

• Return/delete sensitive institutional data if you leave the UM

• Report lost, stolen, or compromised devices

• Allow U-M inspection of your device if an incident occurs

• Produce information as required by FOIA or legal requests
Personal Smartphone/Tablet Responsibilities

• Require a PIN and set lock to 15 minutes or less
• Set to erase data after 10 failed PIN requests
• Turn on Find My Phone/Device
• Use secure wireless connections, such as your dataplan carrier or Mwireless
• Install UM VPN and use it when not using a secure wireless connection (ex: in a coffee shop or hotel) if you are doing university business involving sensitive data
• Keep your software updated
Personal SmartPhone/Tablet Responsibilities
Cont’d….

• Keep your apps updated
• Only install apps from the App store/Play store
• Do not attempt to customize the operating system (no jailbreaking)
• Before selling or giving away your device, back it up and erase all content and settings
• Report security incidents to security@umich.edu

• **Recommended**: Put a sticker on your phone with your name and e-mail address so that you can be contacted if lost.
Personal Computer/Laptop Responsibilities

• Require a password for access to your computer
• Set screensaver to activate after 15 minutes
• Install and use anti-virus software
• Use firewalls and other security software
• Turn on Automatic Updates
• Maintain updates for Chrome and Internet Explorer
Personal Computer/Laptop Responsibilities Cont’d....

• Install encryption for laptops (bitlocker for Win7 and Win8)
• Install and use the VPN client when using unsecure wireless (ex: at a hotel or coffee shop)
• Report security incidents to security@umich.edu
  • Lost or stolen device
  • Malware infection
Remember, its all about sensitive data!

• This only applies if you work with sensitive institutional data on your personal device

THAT SAID....

• All of this guidance also protects YOUR personal information

• Good for YOU...Good for the U(niversity)
Instructions for Securing Your Devices and Data

http://safecomputing.umich.edu/protect-personal/instructions.php

U-M Virtual Private Network

http://www.itcom.itd.umich.edu/vpn/

• Available for desktop/laptops and iOS Apple devices only