Policy on Computer and Mobile Device Security

MICHIGAN
ROSS SCHOOL OF BUSINESS

Purpose

The Stephen M. Ross School of Business at the University of Michigan ("Ross") requires that all individuals accessing any University information resources abide by these security policies established for desktop computers, laptop computers, and other forms of mobile devices, such as cell phones, portable media and others as they evolve. With the increasing use of personal computers and portable devices at the University, there is a growing risk that security vulnerabilities could expose private and confidential data to theft and exploitation. This policy defines a number of safe computing standards to provide protection.

The Community as Partners in Security Awareness

Computing technology is constantly evolving. New hardware devices, software connectivity tools, and data access methods are being developed everyday. Devices are becoming smaller and more mobile. Confidential and private data can be stored, downloaded and shared more easily.

All members of the Ross community have individual and shared responsibilities to protect our information assets in accordance with University policy, and federal, state and local law.

Definition: Sensitive, Confidential and Private Information

Sensitive information refers to information whose unauthorized disclosure may have serious adverse effect on the University's reputation, resources, services, or individuals. Information protected under federal or state regulations or due to proprietary, ethical, or privacy considerations will typically be classified as sensitive. (See SPG 601.27 Information Security).

Securing Your Accounts and Passwords

Users must establish strong passwords and protect passwords from authorized disclosure. The password you select is the cornerstone of all computer security.

- Never give anyone your password for any reason.
- Use letters, numbers and special characters in your password.
- Make sure your password is longer than 8 characters.
- Do not use the same password for everything.
- Always change default passwords.
- Never write your password down.
- Be alert and aware of information stealing methods, such as phishing scams and people watching over your shoulder to obtain personal and sensitive information about you.
- Change your password periodically and immediately if you think it is known by others.
- Refrain from allowing programs and web sites to save your password. This may be convenient, but if you share your computer, or your computer is lost or stolen, others have access to your passwords and accounts.

Securing Desktop and Laptop Computers

Individuals granted access to any Network Resource or Information System will ensure that their desktop and laptop computer is secured from accidental and unauthorized access.

- Computers shall be set to activate the automatic screensaver feature after a period of non-use. The period of non-use shall be for no more than five (5) minutes if the computer contains sensitive or confidential information.
- Users shall only store confidential, sensitive and private information on a networked drive and not on any local disk drive or other portable media that is not properly secured and encrypted.
- Computers and mobile devices that store confidential or sensitive information must use encryption technology at all times, when encryption is available for the device.
- Computers must be turned off or put into sleep mode at the end of each workday.
- Computers must have the current version of anti-virus software installed, with automatic updates, per UM requirements.
- Users must enable the built-in firewall software that is included in major operating systems. A firewall limits the types of connections that other people can make to your computer.
- Users must disable all accounts on the computer or laptop that are not used. Computers can come pre-configured with “guest” accounts that can be easily exploited.
- User must not disable or alter security safeguards installed on desktop or laptop computers, such as virus detection software.
- Users must connect your computer to the Ross network regularly so that critical security patches and software updates can be automatically loaded to your computer.
- Users must dispose of old computers through Computing Services to ensure that all sensitive data is safely removed. Erasing a hard disk does not remove the data effectively.

Physical Security Measures

Physical security measures must be used to secure laptops, computer media, and other forms of information storage media containing confidential or sensitive information.

- Laptop computers actively connected to a Network Resource or Information System must not be left unattended.
- Laptop computers left in a vehicle must not be visible. If possible, the laptop should be stored in a locked trunk. Unattended vehicles shall be locked at all times.
- Laptop computers, computer media and any forms of removable storage (CDs, DVDs, USB keys, flash drives, etc.) must be stored in a secure location (locked cabinet) when not in use.
- Other information storage media containing confidential data such as paper, files, tapes, etc. must be stored in a secure location (locked cabinet) when not in use.

Peripheral Equipment

Peripheral equipment (e.g. printers, faxes, copiers) that store, produce and/or transfer confidential or sensitive information must be protected from inadvertent or unauthorized access.

- Printers, Copiers and Fax machines that print, scan, store or transmit confidential or sensitive information must be placed in secure locations and monitored.
- All documents containing confidential or sensitive information must be cleared from printers and copiers immediately.
- Users must use PIN numbers or use Ross Follow-Me-Printing to send documents that contain confidential or sensitive information to devices in open or public locations.