Facilities Management Procedure
Weber State University
Procedure Number: E01
Issue Date: November 11, 2011
Last Revision Date: November 11, 2011

Security Protocol for Computers in Facilities Management

Description:
This procedure describes the protocol that Facilities Management personnel will follow for the security of desktop and laptop computers.

References:
PPM 10-1 Information Security Policy
PPM 10-2 Acceptable Use Policy
PPM 10-3 Network Security/Firewall Policy
PPM 10-4 Payment Card Handling Policy
PPM 10-5 University Telecommunications Services

Definitions:

Computerized maintenance management system (CMMS): Database that Facilities Management uses as a work management system.

Electronic Communication: Email, text-messaging, instant messaging, and social networks.

Information Technology (IT) Resources: Electronic processing, storage, and transmission systems, which include but are not limited to: computers, terminals, printers, networks, modem banks, departmental information systems copy machines, fax machines, online and offline storage media and related equipment, software, and data files that are owned, managed, or maintained by the University, institutional and departmental information systems, and the University's campus network.
Users: All faculty, staff, administrators, students, consultants, guests, and any person or agency employed or contracted by the University or any of its auxiliary organizations who have a legitimate need to access IT Resources.

**Responsible Party:**

Director of Facilities Business Services or designee

**Procedure:**

Facilities Management (FM) users will act in accordance with University policies to ensure appropriate measures are in place for the security of all desktop and laptop computers in FM. The Director of Facilities Business Services or designee will perform a semi-annual check on all FM computers to ensure required security measures are in place. A preventive maintenance type recurring work request will be entered into the CMMS to prompt this semi-annual review.

The Director of Facilities Business Services or designee will ensure that proper security measures are set up initially for all computers received in FM. Every computer in FM will have the following functions performed in order to maintain the security protocols required by University policy:

**A. Securing Computers**

1. Each computer will be assigned an inventory number. The Systems analyst or the FM employee will report each new computer to Property Control to ensure an inventory number is assigned and the location is recorded for each new computer.
2. Automatic Windows updates will be set to update each time the computer is turned on.
3. Each computer will have an automatic or manual locking system in place when left unattended for any amount of time.
4. Each computer will be turned off at the end of the business day.
5. All “File Printer Sharing” will be turned off at the end of the working period.
6. McAfee antivirus and EPO agents will be updated.
7. Anti-Spyware will be installed and running.
8. All FM employees are required to review and be familiar with Weber State University’s Acceptable Use Policy (PPM 10-2).