POLICY

Effective Date: 1/19/06
Approved By: Director of Facilities Management

Cancels: 98-1

POL-5731.01 FM COMPUTER SECURITY AND DATA MANAGEMENT

This policy applies to all Facilities Management (FM) personnel who use FM computing equipment and resources.

1. FM's Computer Security and Data Management Policy is Established to Maintain Integrity and Security of Electronic Data.

The purpose of this policy is to maintain the availability, integrity and security of documents, spreadsheets, databases, drawings, and other types of electronic data created and used by Facilities Management. employees.

FM has already taken a large step to assure the availability, integrity and security of our data by moving it to the Novell Network System used by the rest of campus. It is imperative that our critical data resides on the Novell System (I: or J: drive, or My Documents folder) which is backed up every night, and not on your local C: drive, which is not backed up. FM's IT staff has the ability to control access to any of our files in the Novell File System in the Facilities Management area.

2. Management of the Computer Equipment and System:

There are 3 web pages provided for all WWU staff for computer use policies:

Administrative Computing (http://www.wwu.edu/depts/admcs/securityWWU.htm) provides a set of Best Practices and Policies for Computer Security and Data Management.

Academic Technology and User Services (ATUS) (http://testwest.wwu.edu/atus/helpdesk/acceptableusepolicy.shtml) provides several web pages related to ethical conduct on our computer workstations.

WWU Interim Policy on Using University Resources (http://www.wwu.edu/policies/docs/5400%20Human%20Resources/POL-U5400.05%20Using%20University%20Resources.pdf) provides information from the state level which talks about using University Resources for personal use.

All FM staff should adhere to these policies where applicable. If your password is discovered by another staff member, contact FM's IT Network Administrator for assistance in changing your passwords.

All FM workstations and servers shall be set up so regular users normally do not have administrator rights. Administrator accounts should be set up for FM's IT staff only.

No personal computer peripheral devices (i.e., PDA's, digital cameras, etc.) shall be installed on your assigned workstation without prior approval from FM's IT Network Administrator. FM will not be responsible to repair or replace any personal devices in use on your FM workstation.

3. Management of the Electronic Data:

FM IT staff will continue to backup all data on the Job Cost server every night of each business day, as long as it remains in service. An off-site copy of Friday's backup will be maintained and traded every other week. Computer Workstations will have their "My Documents" folder pointed to the Novell System under each user's folder in FM_Users by our FM IT staff. All workstations with off-line mail folders (.PST files) will be backed up to the Novell System each day when logging out of Outlook by using Microsoft's tool created for this purpose. The U: drive should be reserved for non-work-related personal files because it can only be accessed through an ATUS staff person if you are not able to login to your computer.

FM IT staff will proactively work on preventing computer viruses from entering any of our servers or computer workstations. All FM staff should immediately notify an IT staff member when a suspicious file is attached on an e-mail or you receive an alert that a file may be infected with a virus – do not open the file.

4. Exceptions:

Energy Management, Fire and Security System applications, databases and documentation used exclusively for building control, fire and security monitoring (which are running on private networks) are under the full control of the Assistant Director of Operations and are excluded from this policy.