

Information Systems Security Guidelines

(OAR 580-055-0050-2B)

The purpose of this section is to define the operational guidelines based on the information classification. The following guidelines are a minimum for people and machines that have access to and/or process information that has been classified by the appropriate Data Steward.

Unrestricted Information:

All computer systems which store or process Unrestricted Information shall have write access restricted only to authorized personnel to ensure that information presented is not edited without appropriate authorization. Any such computer system is also should have fully patched operating systems and applications, and current antivirus software with current virus definitions.

Sensitive Information:

All computer systems which store or process Sensitive Information shall have restricted access granted only to authorized personnel affiliated with EOU, and shall have fully patched operating systems and applications, and current antivirus software with current virus definitions. Any such computer system is also should have fully patched operating systems and applications, and current antivirus software with current virus definitions.

All personnel granted access to sensitive information shall not disclose this information to parties outside of EOU without appropriate authorization by University legal counsel, appropriate Data Steward, or by appropriate EOU leadership.

Protected Information:

All computer systems which store or process Protected Information shall have restricted access to only authorized personnel. Any such computer system is also should have fully patched operating systems and applications, and current antivirus software with current virus definitions.

All personnel granted direct access to Protected Information will be instructed on the proper use and handling of this information as defined by the appropriate Data Steward and will be subject to the Security Sensitive Personnel Policy. Under no circumstances shall Protected Information be disclosed to anybody without authorization from the appropriate Data Steward or university leadership.

All mobile computer systems or portable storage media, which store Protected Information, shall be encrypted with at least the 128bit encryption. Those that can not meet this requirement due to the proprietary nature of how they are created, such as back-up tapes, must be stored in a physically secure area.

April 2, 2008