

# Physical Areas Containing Information Assets Guideline

(OAR 580-055-0050-6A)

The purpose of this section is to outline specific physical security guidelines and procedures which overlap with information security.

## Physical Security:

In general, physical security is the responsibility of Campus Security on campus. The buildings where central servers are housed, office space where Sensitive or Protected Information is regularly accessed and visible to people in the immediate proximity, when electronic storage media is deemed surplus from the university, and where Sensitive or Protected Information is physically transported, as when tape backups are taken off site.

The server room within Inlow Hall and the network room within Pierce Library is to be considered a restricted area where authorized personnel only are allowed. Standard security measures with audited door access codes are employed for physical access to the rooms. Given the critical nature of the Banner systems, the facilities are equipped with standby emergency power (both UPS and generator) and shall be monitored 7x24 for availability.

## Paper Security:

Paper documents that include Sensitive Information or Protected Information like Social Security numbers, student education records, medical benefits, compensation, loans, financial aid data and personnel evaluations are to be secured during printing, transmission (including by fax), storage, and disposal. University employee and supervisor responsibilities include:

1. Do not leave paper documents containing Protected Information or Sensitive Information unattended; protect them from the view of passers-by or office visitors. Store paper documents containing Protected Information or Sensitive Information in locked files, with documents critical to business operations in a fireproof safe with copies in an alternate location.
2. Do not leave the keys to file drawers containing Protected Information or Sensitive Information in unlocked desk drawers or other areas accessible to unauthorized personnel.
3. All records are subject to OUS records retention policies and should be only be disposed of in accordance with the retention schedule defined within those policies. Once the retention schedule has been met, shred confidential paper documents and secure such documents until shredding occurs.

April 3, 2008