Policy No. 812
Area: Information Technology Services
Adopted: 8/6/2012

Information Security Operational Procedures
Physical Access Security Policy

BACKGROUND

Technology is capable of addressing many threats, but physical security measures are also required to address any non-technical threats to information, equipment, and the infrastructure.

POLICY

University information may be stored in any form including but not limited to, paper copies, disks, USB drives, tape, CDs, DVDs, and hard disk drives. All forms of information are subject to physical threats such as theft, malicious damage, vandalism, or errors. Each unit or individual responsible or in possession of University information will secure that information to a reasonable and prudent level regardless of its current form using an access control mechanism. Each unit will detail who within that unit has authority to access private data and a detail log of sensitive information will be kept by the unit's security contact.

Units responsible for enterprise information or services must be vigilant in securing access to facilities housing services as well as the utilities (electricity, gas, generators, etc.) servicing the facility. These units should log visits to the facilities, and log who has keys, swipe cards, proximity cards, etc. that allow entry to the room and any utilities servicing the unit. Locations housing critical infrastructure shall be secured from all non-support entities so as to limit the potential for damage from outside sources.

RESPONISBILITIES

Desktop computers, laptops, handhelds, USB drives all can hold information that should not be public. Modern technology continues to strive to make these devices smaller, lighter, and more powerful making it far easier to steal them. Common sense and a good lock are the best deterrents to most physical threats. Computers or devices left unattended in an open office or

classroom are prime candidates for theft or malicious mischief. Equipment and confidential information shall be in a locked facility when not currently being used.

Server rooms and network closets shall be for the exclusive use of the Division of Information Technology & Services (ITS). The facility shall be accessible only to approved IT staff or those approved by the CIO or designee. All access to these rooms should be supervised and logged.