PHYSICAL AND ENVIRONMENTAL SECURITY
07.300.03

Authority:	Chief Information Officer (CIO)
History:	Approved by CIO July 10, 2021
Sources of Authority:	UNC System Office Policy Manual, Chapter 1400 "Information Technology"; International Organization for Standardization ISO/IEC 27002
Related Links:	07.100.00 Responsible Use of Information Technology Resources 07.200.00 Responsible Management of Information Technology Resources
Responsible Office:	Information Technology Services

I. Purpose

The purpose of this policy is to establish standards for the prevention of unauthorized physical access, damage or interference to the university's information and information processing facilities. The university prioritizes the prevention of loss, damage, theft, or compromise of assets and has put in place this policy in order to minimize possible interruption to the university's operations.

II. Definitions

A. Physical Access Controls: the installation of either a passive or active hardware restraint, or other appropriate prevention measure.

III. Policy

A. Secure Area Controls

1. The physical access controls to locations which house information resources must be documented and maintained in a secure location.
2. Access to physical locations which house critical infrastructure must be limited to individuals with explicit need.
3. All information processing facilities must be protected by physical controls that are appropriate for the size and complexity of the operations and the criticality, sensitivity, regulatory compliance requirements, and risks to the systems or services operated at those locations.
4. In areas with a high level of sensitivity, visitors must be required to sign in and be wearing an identifiable badge which denotes their status as a visitor.
5. Risk assessments must be conducted periodically to review the effectiveness of physical security and emergency procedures.

B. Asset Removal and Data Destruction

1. Entry points (access/egress), such as delivery and loading areas, and other points where unauthorized persons could enter the premises should be controlled, and if possible, isolated from information processing facilities.
2. Identification must be provided to individuals who have been given the authority to remove assets from campus to an off-site location.
3. All university data storage or processing devices will be examined prior to disposal or transfer to surplus and, if needed, processed, in order to assure that no institutional or protected data, proprietary software or software not licensed to be transferred with the computer resides on media attached to the device.
4. Removal of institutional or protected data, proprietary software or software not licensed to be transferred with the computer will be accomplished by use of ITS Security approved data destruction process or by physical destruction of the media.
5. All university computers that contain, or have contained protected data, proprietary software or software not licensed to be transferred with the computer will be certified as sanitized per ITS Security approved process prior to disposal or transfer to another department or work unit.
6. Building entrances and exits to critical infrastructure and equipment will have surveillance mechanisms in place to monitor incoming and outgoing traffic.
7. Network and server infrastructure is not to be taken off site without explicit approval from the CIO.

C. Equipment Resiliency and Protection

1. Designated areas that are designed to minimize risks from natural disasters or other hazards must be used to house sensitive equipment.
2. Measures relating to the protection of sensitive data or critical university equipment from physical harm or compromise must be established, documented, accessible and tested on a periodic basis.
3. All facilities housing servers and/or network appliances will have, where appropriate, fire sensing/extinguishing devices present.
4. Designated employees shall be trained to monitor environmental control procedures and equipment and shall be trained in desired response in case of emergencies or equipment problems.
5. Where appropriate, redundancy for equipment used to provide critical service must be maintained.

D. Clear Desk and Clean Screen

1. If a computer that processes sensitive data or critical university business information is left unattended or is no longer in use, the user session must be locked or terminated.
2. All spaces housing computers or equipment that process sensitive data or critical university services should be kept locked when not occupied by the employee(s).
3. Portable devices used in openly accessible areas should be locked in secure cabinets when not in use. Offices containing portable devices should be locked when not occupied.

4. All sensitive data in written format, including login credentials, must be stored in a locked cabinet or safe when unattended.

5. Efforts must be taken to ensure monitors and displays which may contain university owned sensitive data are not visible to anyone other than the intended user. Configuration of offices, desk locations, monitor orientations and window placement should be taken into consideration when setting up office space.