East Georgia State College
Physical Security of Information Technology Resources Policy
Adopted by President’s Cabinet 7/27/21

1.0 Background
Physical security measures are an important part of any effort to protect the confidentiality, integrity, and availability of information assets and services. Adequate physical security is critical to the success of all other information security measures. Without physical access control there can be no protection from unauthorized use of computing resources and without physical environmental control, equipment is prone to theft, unpredictability, and failure.

2.0 Purpose
The intent of this policy is to protect East Georgia State College’s (EGSC) computing resources from unauthorized physical access and environmental harm. The policy establishes guidelines and best practices for controlling the physical environment where computing resources reside. Computing resources include, but are not limited to, personal computers, printers, file servers, routers, data switches, cabling, and the associated space where equipment resides.

3.0 Policy

Physical Access:

• All data centers, data closets, and computer labs, must remain locked when not in use and any devices critical to the College’s network must be located in lockable dedicated rooms.

• Access to data centers, campus data closets and restricted areas of EGSC Information Technology must be limited to authorized EGSC personnel by means of a proximity card access system or other lock measures. Only those personnel requiring access to perform their duties can be granted right of entry.

• Employees must lock offices and work areas that contain computer equipment or sensitive information.

• Employees must coordinate the relocation of any type of computer equipment with EGSC IT personnel for proper maintenance of inventory records.

• Report suspected theft, damage, or destruction of computer equipment anywhere on campus to the EGSC IT Help Desk and the EGSC campus Police Department.

Environmental Controls:

• All data centers, data closets, computer labs, must remain equipped with environmental controls also any other devices that supports the College’s network must be located in dedicated rooms equipped with appropriate environmental controls.

• Temperature and humidity should be regulated and monitored and fire suppression equipment installed or readily available.
• Critical equipment such as file servers, routers, and data switches must connect to Uninterruptible Power Supply (UPS) units.

• 4.0

Procedures and Responsibilities

• Employees are responsible for physically safeguarding the computer equipment in their offices and departmental spaces.

• EGSC’s IT Department maintains sole authority over the EGSC network infrastructure and all computing resources. Authorized EGSC IT personnel have physical access to data centers, data closets, computer labs, offices, and any other location where computing equipment resides based on job requirements.

• EGSC IT personnel may request keys as necessary to gain access to campus buildings and the rooms containing computing resources. Personnel must adhere to the facilities procedure for obtaining keys and must safeguard the keys at all times.

• Restricted EGSC IT areas include the data center, administrative computing and networking services, and data closets.

The following applies to these areas:

• Entrance doors feature a proximity card access system, punch lock, or key lock.

• The Information Technology Department is responsible for granting access to these areas and managing cards and documentation.

• Contractors and other third parties must show ID, have the purpose of their visit verified, and be escorted by authorized personnel. If a contractor needs repeated access throughout the day, the Information Technology Department may issue them a temporary access card. There is also a visitor log that includes date and time that must be signed each time a visitor enters EGSC IT Department restricted areas.

• EGSC employee ID Cards that are lost or stolen must be immediately deactivated as well as the ID card assigned to an employee who ends employment with the college.