Policy Title:	Open Computer Lab and Classroom Technology Policy
Issue Date:	July 7, 2007
Effective Date:	September 1, 2015
Last Reviewed:	August 1, 2015
Responsible Office:	Vice President for Operations and Chief Information Officer/Chief Business Officer
Contact Information:	University Information Technology Services/ Information Security Office Phone: 470-578-6620 Email: iso@kennesaw.edu

1. Purpose Statement

This policy defines usage requirements for Kennesaw State University (KSU or the University) open computer labs and technology classrooms. Through the utilization of the safeguards described herein, these classrooms and labs support the mission of the University while also protecting the physical and logical assets contained therein.

2. Background

The KSU Open Computer Lab and Technology Classroom Policy was created to comply with the University System of Georgia information technology policies. Pursuant to the University System of Georgia (USG) *Information Technology Handbook*, Section 5.1.2, KSU is required to establish and maintain "appropriate internal policies, processes, standards, and procedures for preserving the integrity and security of each automated, paper file, or database."

3. Scope

The Open Computer Lab and Technology Classroom Policy applies to all KSU employees (faculty and staff) and students authorized to use, maintain, or design a KSU open computer lab and/or a technology classroom. This policy supplements, and works in conjunction with, existing University policies published in the KSU *University Handbook* and available at policy.kennesaw.edu .

4. Exclusions or Exceptions

Environmental factors, including but not limited to heat and fumes, may necessitate the opening of doors that are typically secured. In these instances, KSU maintenance should be notified of the issue and the doors re-secured after the room is vacated.

PC over IP (PCoIP) labs are fundamentally different in architecture than traditional open computer lab environments, based on the absence of local storage and the reduced hardware cost. Based on these factors, PCoIP Labs are excluded from this policy.

Exceptions to the KSU Open Computer Labs and Technology Classroom Policy may be granted only via approval from the vice president for Operations/CIO.

5. Definitions

Definitions are available via the IT Glossary on the KSU policy website at policy.kennesaw.edu.

6. Policy

All KSU open computer labs and technology classrooms must meet the applicable requirements outlined in this document. These requirements define operational and technical security safeguards that maximize accessibility while also protecting university technology assets. In some circumstances, lab areas may be located in campus common areas that are difficult to secure due to lack of a confined space. In these instances physical security safeguards, including but not limited to locks, security cables, video surveillance, and locking cabinets are recommended to mitigate the threat of physical theft.

a. KSU Open Computer Lab Requirements
   1) All open computer labs must be managed in accordance with all applicable university policies and procedures.
   2) All open computer labs must be monitored by an authorized KSU employee and locked when monitoring is not available or in use.
   3) No student, except those employed by the University, may be left alone in an open computer lab.
   4) All open computer labs must be secured with an auditable locking door that is also used to gain individual entry to the lab. All other doors must remain externally locked at all times.
   5) Campus departments are responsible for all applicable procedures for their respective open computer labs that align with this policy and the Lab and Classroom Technology Standard.

b. KSU Technology Classroom Requirements
   1) All technology classrooms must be managed in accordance with all applicable university policies and procedures.
   2) All technology classrooms must be vacated and locked when class is not in session or a responsible/designated KSU employee is not present.
   3) All technology classrooms labs must be secured with an auditable locking door that is also used to gain individual entry to the room. All other doors must remain externally locked at all times.

7. Associated Policies/Regulations

   a. USG *Information Technology Handbook*, 5.1 Information Security Program
   b. Exception Request Form: Open Computer Lab and Technology Classroom Policy

8. Procedures Associated with this Policy

   a. Lab and Technology Classroom Standard

9. Forms Associated with this Policy.

   a. As required by information in Sections 7 and 8.

10. Violations

Any open computer lab and/or technology classroom found to be in violation of this policy will be disconnected from the campus network without notice and may result in disciplinary action. In the event of a security violation, the department responsible for the affected lab and/or classroom is responsible for all technology replacement costs.

11. Review Schedule

The Open Computer Lab and Technology Classroom Policy is reviewed annually by the Office of the Vice President for Operations/CIO or his/her designee.