Auburn University at Montgomery
Policies and Procedures

Title: Computer Authentication Policy

Responsible Office: Information Technology Services (ITS)

I. PURPOSE

The purpose of this policy is to ensure the security, confidentiality and appropriate access and utilization of Auburn University at Montgomery (AUM) computer systems and data.

II. POLICY

AUM computer systems will be configured to require authentication at startup. When possible, authentication will be done through official domain facilities; otherwise, authentication will be established on each individual device.

AUM computer systems will be configured to have a screen lock that engages after no more than 30 minutes of inactivity, and which requires re-authentication. When possible, the screen lockout will be controlled through official domain group policies. Screen lock duration will depend on the role of the computer systems but shall not exceed the 30-minute limit.

III. EFFECTIVE DATE

May 1, 2023

IV. APPLICABILITY

This policy applies to all university computers with exclusions listed below.

V. RESPONSIBILITY

ITS implements and administers the policy/procedure in detail.

Policy Responsible Office: Information Technology Services
Policy Responsible Executive: Chief Information Officer (CIO)

VI. DEFINITIONS

N/A

VII. PROCEDURES

- ITS administrators, college/school/department system administrators, and/or individual users with administrative authority are responsible for ensuring that appropriate authentication procedures are in place.
- Individuals accessing AUM computer systems, or who have the ability to access AUM confidential information on any computer or system must log off, lock their devices or otherwise secure their devices when such devices are left unattended.
- When confidential information can be accessed such as credit card information, Protected Health Information (PHI), FERPA protected information, or human

resource records, it is recommended that the inactivity period be set as low as possible, typically 15 minutes or less or as required by applicable compliance frameworks.

- When possible, the screen lockout will be centrally controlled by ITS.

VIII. SANCTIONS

First occurrence: A notification of noncompliance and to remediate is made to the individual with administrative authority for the machine to bring into compliance. Any circumstances where such computer system is not or is unable to be brought into compliance must be reported to ITS immediately.

Second occurrence: A second notification of noncompliance and to remediate is made to the individual with administrative authority for the machine to bring into compliance. ITS may also notify the individual's supervisor.

Subsequent occurrence: Administrative privileges and/or access to systems may be discontinued until the computer system is in compliance. Other disciplinary sanctions may be implemented in accordance with applicable conduct policies.

IX. EXCLUSIONS

Public classroom computers (Instructor Controlled Devices) require authentication but may be exempted from the 30-minute lockout requirement, but with a maximum time set of 100 minutes.

Machines with a requirement for public access and that are configured to have limited ability to store or access confidential information to the device or the network are excluded from this policy. Public access machines in the library are examples of such machines.

The CIO has the authority to exclude computers from this policy and may add constraints to those exclusions. Individual colleges/departments may choose to implement a shorter screen lockout interval.

X. INTERPRETATION

The AUM Chancellor has the authority to interpret this policy.

APPROVAL TO PROCEED: ____________________ **DATE:** 4/18/23

APPENDICES

NONE