Computer Authentication Policy

I. POLICY STATEMENT

Auburn University computers will be configured to require authentication at startup and a screen lock after a period of inactivity.

II. POLICY PRINCIPLES

For the security of the Auburn University network, the protection of Auburn University data and the maintenance of privacy and confidentiality of information stored on Auburn University computers, it is important to ensure that only authorized users have access to AU computers.

III. EFFECTIVE DATE

Adopted 04/13/2007
Revised 04/30/2016

IV. APPLICABILITY

All university computers - see Exclusions below

V. POLICY MANAGEMENT

Responsible Office: The Office of the CIO
Responsible Executive: Chief Information Officer
Responsible Officer: Information Security Officer

VI. DEFINITIONS

VII. POLICY PROCEDURES

a. College/school/department system administrators, administrative units and/or individual computer owners with administrative authority are responsible for ensuring that appropriate authentication procedures are in place.

b. Authentication will be controlled through centrally maintained capabilities when possible; otherwise, an authentication procedure will be established on the individual machine.

c. Individuals accessing Auburn University computers or accessing AU confidential information on any computer should log off or lock their computers whenever computers are left unattended.

d. Auburn University computers will be configured to have a screen lock that engages after no more than 30 minutes of inactivity and that requires re-authentication.

e. When sensitive information can be accessed such as personal credit card, 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.

f. For computers with access to sensitive data in public areas (e.g. Registrar's office) that are easily accessible by non-authorized users, a lower inactivity timeout is recommended.

g. When possible, the screen lockout will be controlled through the centrally maintained authentication system.

h. The Office of Information Technology will supply documentation for configuring authentication on all supported operating systems.

i. Individual colleges/schools/departments, administrative units and individuals may choose to implement a shorter screen lockout interval.

j. When a computer that is not in compliance with this policy is discovered, the Information Security Officer (ISO) will notify the college/school/department system administrators, administrative unit and/or individual computer user with administrative authority and will request that (1) proper authentication procedures be put in place and (2) the ISO be notified when this is completed. The ISO will warn that additional sanctions will occur if the request is not honored.

k. If the computer remains out of compliance after seven days, the Information Security Officer will notify the college/school/department system administrators, administrative unit and/or individual computer administrative authority and their managers and will request that (1) proper authentication procedures be put in place within the next three days and (2) the ISO be notified when this is completed. The ISO will warn that if the second request is not honored, the computer will be disconnected from the network until it is in compliance.

l. If the second request is not honored, the Information Security Officer may direct that the computer be disconnected from the network until its compliance with this policy is verified.

m. Based on a risk analysis of the Probability and Impact of Data disclosure, the Information Security Officer can request that a machine be moved to a physically secure location.

VIII. SANCTIONS

a. Deliberate disregard of this policy or the protection standards created to implement this policy will be considered a Group I infraction under the University Personnel Manual and is subject to disciplinary action, up to and including dismissal.

IX. EXCLUSIONS

a. Public classroom computers (Instructor Controlled Devices) require authentication, but may be exempted from the 30-minute lockout requirement.

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

c. The Information Security Officer has the authority to exclude computers from this policy and may add constraints to those exclusions.

X. INTERPRETATION

The Chief Information Officer and the Information Security Officer have the authority to provide interpretations of this policy.