Computer Authentication Policy

I. PURPOSE
To ensure that only authorized users have access to Auburn University computers.

II. POLICY
Auburn University computers 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 machine.

Auburn University computers 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.

III. APPLICABILITY
All university computers - see Exclusions below

IV. RESPONSIBILITY
OIT and College/School/Department system administrators and/or individual computer owners with computer administrative authority.

V. DEFINITIONS

VI. PROCEDURES
OIT and College/School/Department system administrators will provide instruction to configure all supported operating systems.

VII. SANCTIONS
First offense: A request is made to the individual with administrative authority for the machine to bring it into compliance, and to convey subsequent sanctions.

Second offense: A request is made to the individual with administrative authority for the machine to bring it into compliance, and to convey subsequent sanctions, manager cc’d.

Subsequent offenses: Machine is disconnected from the network until in compliance.

VIII. EXCLUSIONS
Exclusions will be determined by the OIT or distributed IT staff. Excluded machines should be locked down to the extent possible while continuing to provide the necessary functions.

Machines with a requirement for public access where physical access is controlled/monitored or the machines are configured to have limited access to the network – e.g. Public access machines in the Library.

Machines in a classroom environment, physical access should be controlled or monitored. Machines configured for group access which have a common logon. Physical access should be controlled or monitored and/or network access restricted.

Individual College/School/Departments may choose to implement a shorter screen lockout interval.

IX. INTERPRETATION
CIO, Executive Director OIT

FINAL APPROVAL: Executive VP, Provost, Banner Executive Committee
ADOPTED: 04/13/2007