Endpoint Protection Policy

I. POLICY STATEMENT

All endpoint devices including laptops, desktops, and mobile devices connected to the Auburn University Network or which access University data must meet endpoint standards.

II. POLICY PRINCIPLES

The key principles of this endpoint policy are the prevention of endpoint virus outbreaks and the assurance that Auburn University employees, students, and affiliates are aware of their responsibility to protect the endpoints connected to the Auburn University Network.

Auburn University has developed Minimum Endpoint Protection Standards that university-owned devices must meet.

All computers (student and employee) connected to the Auburn University Network or storing Auburn University confidential or operational data must be protected by current anti-virus software.

III. EFFECTIVE DATE

November 15, 2017

IV. APPLICABILITY

This policy applies to all endpoint devices with access to the Auburn Network.

V. POLICY MANAGEMENT

Responsible Office: Office of the CIO
Responsible Executive: CIO
Responsible Officer: Executive Director, IT

VI. DEFINITIONS

None.

VII. POLICY PROCEDURES

None.

VIII. SANCTIONS

Deliberate violation of this policy is subject to disciplinary action, up to and including dismissal.

IX. EXCLUSIONS

None.

X. INTERPRETATION

Office of the CIO