Software & Information Technology Services Approval Policy

I. POLICY STATEMENT

Review and approval are required prior to the acquisition or renewal of any software or information technology services to ensure they meet or exceed regulatory statutes and best practices.

II. POLICY PRINCIPLES

The review will include, as applicable, compliance with Auburn's Electronic and Information Technology Accessibility Policy, various other policy and compliance requirements (HIPAA, FERPA, etc.), and best practices to protect the confidentiality, integrity and availability of information through an appropriate information security controls review.

An approval process has been established that ensures review by the appropriate offices, including the Office of Accessibility, the Information Security Office, the Division of Institutional Compliance & Privacy Office, the Office of Cash Management, and the Office of Information Technology (Vetting Group).

The Vetting Group (Vetting@auburn.edu) within the Office of Information Technology must be contacted prior to the creation and dissemination of any requisition or request for proposal (RFP) for software or information technology services. This policy applies regardless of the means of acquisition, such as purchasing card, requisition, or gift.

This review process evaluates the security controls available from the vendor, but not how the controls are implemented by Auburn University. To that end, security implementation assistance is available from the Information Security Office. When deemed appropriate by the Chief Information Security Officer, a security controls review, and final approval will be required prior to use.

Vetting third-party service providers to the institution as "capable of maintaining appropriate safeguards" and requiring them to do so by contract will be part of this review.

Although a software or information technology-related service may have been through the review process, the software was approved for a specific scope of use. Further evaluation and approval may be required if the scope of use is changed or expanded, such as use by a different department or a use that expands the number of users.

The Office of the CIO maintains a list of hardware that contains a software component, software and IT services which has been vetted and software available for download.

Information Technology Services does not include contracted professional services, but does include cloud services that store or maintain Auburn Data.

These policies and procedures apply to all university purchases of information technology software and services at Auburn University. This includes hardware which has a software component that processes or stores PII.

III. EFFECTIVE DATE

November 10, 2017
Revised: November 21, 2019

IV. APPLICABILITY

This policy applies to all Auburn University employees, students, and agents.

V. POLICY *MANAGEMENT*

Responsible Office: The Office of the CIO, the Chief Financial Officer, and the Division of Institutional Compliance & Privacy Office
Responsible Executive: Chief Information Officer (CIO)
Responsible Officer: Chief Information Security Officer (CISO)

VI. DEFINITIONS

ADA – Americans with Disabilities Act
FERPA - Family Educational Rights and Privacy Act
HIPAA - Health Insurance Portability and Accountability Act
PBS – Payment and Business Services
PCI DSS – Payment Card Industry Data Security Standards
PII – Personally Identifiable Information
RFP – Request for Proposal
Information Technology Services are human resources and technology that provide for the storage, computing, distribution, and communication of Auburn Data.
Software is the entire set of programs, procedures, and related documentation associated with a computer system,

VII. POLICY PROCEDURES

The process begins by submitting an internal product questionnaire through AU Vetting(Vetting@auburn.edu) within the Office of Information Technology (OIT)
All software and IT services must request vendors complete the appropriate Auburn University Questionnaires (e.g. Information Security Questionnaire, PCI Questionnaire, and Product Accessibility Questionnaire), it is suggested that all RFPs include the questionnaires.

The Information Security Group will also accept the Higher Education Community Vendor Assessment Tool (HECVAT) which was created by the Higher Education Information Security Council (HEISC) in collaboration with Internet2 and REN-ISAC.

VIII. SANCTIONS

Deliberate violation of this policy by employees may subject them to disciplinary action, up to and including dismissal.

Software and information technology services acquired without this review may be removed from Auburn University computers or access restricted.

IX. EXCLUSIONS

None

X. INTERPRETATION

The Office of the CIO

APPENDICES

Attach a full version, in PDF format, of the submitted policy and supporting documents (i.e. forms, exhibits, memorandums etc.)