

Area of Responsibility: BUSINESS INTELLIGENCE AND TECHNOLOGY

Responsible Contact: DIRECTOR

Policy Identification: VENDOR MANAGEMENT

Effective Date: DATE (Revised: 08/15/2019)

**PURPOSE**

To specify security requirements for the acquisition of information technology products and services in which the Universitydata is stored, processed or transmitted by an entity not under control of the university. This covers outsourced services, server hosting, Managed Service Providers (MSPs), Software as a Service (SaaS), and “Cloud” computing services.

**POLICY**

1. Service Agreements will address the following topics to the satisfaction of the university, based upon the needs of the project:
   1. Availability
   2. Data preservation and destruction after termination of service
   3. Backups
   4. Intellectual property considerations
   5. Remedies for failure to perform
2. External IT Vendors that will store, process or transmit Restricted Data must:
   1. Sign a Data Security Agreement stating their responsibility to protect the university data; comply with all university security policies and standards, as well as applicable laws and regulations; screen and monitor personnel; and specifying legal liability.
   2. Provide external validation of the vendor’s compliance with required controls. This validation can consist of a reliable third-party audit, certification, attestation, or an assessment conducted by the university.
3. Periodic review of vendor’s controls and continued compliance will be conducted as needed, based upon significant changes to the use of the system, system design or controls, and at least every two years for projects that store, process or transmit restricted data and every three years for all other projects.
4. Documentation of evaluations, assessments and reviews must be retained according to university records retention schedules and applicable laws.

able)