UF UNIVERSITY of FLORIDA
Information Technology

Standard: External IT Vendor Sourcing

Purpose:

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

Standard:

1. Service Level Agreements will address the following topics to the satisfaction of the university, based upon the needs of the project:
   a. Availability
   b. Data preservation and destruction after termination of service
   c. Backups
   d. Intellectual property considerations
   e. Remedies for failure to perform
2. External IT Vendors that will store, process or transmit **Restricted Data** must:
   a. Sign a Data Security Agreement stating their responsibility to protect University of Florida Data; comply with all UF Security Policies and Standards as well as applicable laws and regulations; screen and monitor personnel; and specifying legal liability.
   b. 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. External IT Vendors that will store, process, transmit or otherwise have access to Protected Health Information must sign a Business Associate Agreement.
4. 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..
5. Documentation of evaluations, assessments and reviews must be retained according to university records retention schedules and applicable laws.

References:

SEC-RM-001: Information Security Risk Management Policy