Policy

Title:	**Technology Vendor Management**
Effective Date:	November 8, 2022
Approved By:	President's Council
Responsible Party:	Vice-President for Technology & Learning Services (TLS)
History:	N/A
Related Documents: N/A	

I. PURPOSE

Salus University utilizes third-party Information Technology (IT) vendor products and services to support its mission and goals. This IT Vendor Management Policy contains the requirements for how Salus University will preserve and protect information when using third-party IT vendor products and services.

II. DEFINITIONS

Third party IT vendor – Person or company that provides Information Technology (IT) products or services under contract for Salus University

HIPAA – Healthcare Insurance Portability and Accountability Act

FERPA – Family Educational Rights and Privacy Act

PCI DSS - Payment Card Industry Data Security Standard

BAA – Business Associate Agreement

III. POLICY

Salus University's management of third party IT vendors is part of its overall risk management. To ensure full compliance with applicable law and regulations regarding risk management, IT vendor management, contract management and management of third-party service providers Salus University must follow the guidelines and procedures stated in this policy.

A. University Management Compliance

1. New Product or New Service:

- Establish service or product needed.
- Identify vendors who can provide needed service or product.
- Prepare a Request for Proposal (If required).

- Perform due diligence review as required (See IT Vendor Due Diligence below).
- If necessary, request vendor presentations for the finalists.
- HIPAA, FERPA and PCI DSS related software may require BAA be executed.
- Execute the primary contract.
- Proceed with implementation that includes the following:
  - Timeline for implementation.
  - Impact on TLS and University personnel resources during implementation.
  - Policies and procedure development, revision or deletion including communication of such changes.
  - Training scheduled/completed, as required.
  - Execution of Warranty and maintenance schedules.

2. Request for Proposal

- The timeframe for completing and distributing RFPs (if required) will be directed by TLS in conjunction with the appropriate academic or programmatic department.
- Once RFPs have been returned by the vendors, TLS or assigned staff will schedule meetings to review proposals and select a vendor.
- The timeframe for review and selection of a vendor will be directed by TLS and the related college or department.
- The vendor(s) selected will be subject to the required due diligence review.

3. IT Vendor Due Diligence

- With consultation from the applicable College or department administration, TLS will evaluate all vendor products and services, negotiate the cost and negotiate the contract terms before contracting with the vendor. The type of evaluation will vary and should be commensurate with risk, complexity and product or service cost.
- Verbal product and service agreements are prohibited. All IT vendors must provide a written contract and/or service agreement.
- TLS will appoint, as needed, appropriate staff members to perform a due diligence review prior to entering any arrangement with a third-party vendor and due diligence reviews for existing third-party vendors.
- TLS will create and maintain a list of all established vendors and contracts that are current contracts and active.

4. On-going Oversight of Third-Party Vendors

- TLS will have the responsibility for the management of the vendor(s) relationship(s) unless assigned to another party by University administration.
- TLS will provide review and oversight for current contract(s) along with the supporting due diligence to determine if any new or outstanding issues exist.

- TLS will record the results of any oversight reviews for the third-party services to determine the appropriate action for any issues that may be present.
- Appropriate action is defined as one of the following:
  - Approval to continue service with vendor;
  - Approval to continue service with the vendor, but on conditions of additional information and/or more frequent review;
  - Begin a process to review other vendors; or
  - Terminate the service/product contract with the vendor.

5. Legal Review Standards

- Legal review is required for all agreements, additional actions may be required in the event of one or more of the following conditions arises:
  - The vendor is in the process of merger or acquisition of its services causing potential business interruption or unwanted changes to its contracted services.
  - The vendor refuses to implement recommended changes to existing contracts(s) or other identified risk(s) within their business practices.
  - Failure of the vendor to meet the terms of the contract.

6. Contract Standards Checklist Guide

- Service or product definitions and service level expectations (performance and reliability standards).
- Technology specifications and operational responsibility.
- Confidential Information privacy and security.
- Vendor reporting and documentation and audit rights.
- Business continuity and disaster recovery reporting and standards.
- Subcontract and third-party responsibility and liability.
- Statement of compliance for the following:
  - A signed BAA if necessary.
  - Detailed fee structure and billing terms.
  - General terms: liability limitations, recourse, warranties, arbitration, termination, contract expiration, assignment, and indemnification.

7. Reporting and Documentation Standards

TLS will maintain documentation for each vendor including a fully signed contract with all service level agreements and addenda, non-disclosure agreements, BAA, confidentiality agreements or invoices, together with a completed contract checklist including the following:

- Vendor due diligence documentation.
- Material communications such as disputes, contract changes, fee changes, service, or performance issues.
- Due diligence checklist.
- Completed Risk Assessment as required.

8. Relationship Monitoring Standards

TLS assigns a vendor risk rating at the time of engagement and is reviewed periodically through the term of the contract. TLS will determine the level of IT vendor risk based upon the following criteria:

- **Criticality:** Impact to operations if the service or product was suddenly not available.
- **Dependence:** Degree of difficulty involved in finding and implementing a service or product replacement.
- **Financial Commitment:** Higher financial commitment equates to higher risk of monetary loss if relationship were to fail.
- **Performance:** Vendors with substandard or unproven performance require a higher degree of monitoring by TLS.
- **Regulatory Impact:** Assurance vendor is compliant to and will provide on-going adherence to required State, Local and Federal Regulations.
- **Business Impact** reputation or strategy.

9. Vendor Types Subject to Initial and On-Going Due Diligence

- Electronic Health Records and Diagnostic Systems
- Student Services Software
- Financial accounting and management services (Accounting, payroll, fund raising and alumni)
- Human Resources Information Management Software
- Learning Management Systems
- General administrative systems (copiers/printers, building access & security, room scheduling)
- Academic program systems (e.g. student clinical experience software, testing software)
- Research Software
- Network Security Support Systems
- Phone Systems
- HVAC Systems