Operating Instruction 5.23.1.14 Review of Third Party Vendors

Part 1. Purpose
To establish minimum requirements for the oversight and monitoring of any third party vendor that handles, processes or stores enterprise system data that is classified as Highly Restricted or Restricted data as defined in System Procedure 5.23.2 Data Security Classification and Operating Instruction 5.23.2.1 Data Security Classification.

Part 2. Definitions
For purposes of this operating instruction, the following definitions apply:

Business Owner
Any Minnesota State employee delegated the authority for ensuring due diligence prior to the execution of a contract; managing the third party relationship and/or monitoring service delivery for compliance with federal and state laws, regulations, Minnesota State Board Policies, system procedures, operating instructions, and/or contract agreements.

Enterprise system data
Minnesota State electronic data collected, stored, transmitted or maintained by the system office, or a third party acting on behalf of the system office for the benefit of the colleges and universities within the Minnesota State system.

Service Organization Control (SOC) reports
Report(s) on a third party's controls that are relevant to security, availability, processing integrity, confidentiality or privacy, and the customer's internal control over financial reporting. These reports are intended to meet the needs of a broad range of customers that need detailed information and assurance about the effectiveness of the third party's controls.

Statement(s) on Standards for Attestation
A regulation created by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) for defining how service organizations report on compliance controls. The regulation requires the management of the service organization to provide a written assertion to the auditor that their description accurately represents their organizational system. The organization's system description consists of the services provided by the organization and all operational activities that affect the service's customers. In addition, the organization must also assert that their description honestly

describes their control objectives and the time period in which they are meant to be evaluated.

Part 3. Due Diligence Prior To Contract or Agreement Execution or Renewal

For any systemwide service provided by a third party vendor that handles, processes or stores enterprise system data that is classified as Highly Restricted or Restricted data, prior to the execution or renewal of a master contract, the security controls and data management practices of the vendor must be reviewed to ensure Highly Restricted and/or Restricted data will be adequately secured. The Business Owner shall conduct the review in consultation with the system office Information Security, Risk, and Compliance department.

The Business Owner is responsible for obtaining any necessary review and approval of the contract by system legal counsel, as required by Board Policy 5.14 Contracts and Procurements.

Part 4. Annual Review of Control Environment

The Business Owner shall consult with the system office Information Security, Risk, and Compliance department to conduct an annual review of the controls, data management, and security practices of the third party vendor.

To ensure the controls adequately protect Highly Restricted and/or Restricted data, the following documents must be reviewed:

- The original contract and any applicable addendums, exhibits, or attachments;
- If available, the vendor's Service Organization Control (SOC) reports;
- Any other report that has been conducted by a third party that evaluated the third party's data management and/or security controls. This does not include the third party conducting an internal evaluation of their own controls or practices.

The review must also include an evaluation of controls performed by Minnesota State that are required by terms in the contract or agreement with the third party. If a SOC report is provided by the vendor, the controls that must be implemented by Minnesota State will be identified in the report as "complementary user entity controls."

Part 5. Documentation of Annual Review

The results of the annual review of the control environment must be documented and retained by the Business Owner in accordance with records retention schedules. Documentation must include:

- Business Owner name and title;
- Vendor or company name, or the college, university or system office that is providing the service;
- Brief description of the service provided;
- Date of original contract or agreement;

- Any and all documents or reports (e.g., Service Organization Control reports, Statement(s) on Standards for Attestation, etc.) that were included in the review process;
- Any deficiencies in the third party's data management practices – i.e., data backup practices, comingling with other customers' data, sharing data with other third party entities, etc.;
- Any deficiencies in the third party's security controls, as identified by the system office Information Security, Risk, and Compliance department;
- Any deficiencies in Minnesota State's security controls, as identified by the system office Information Security, Risk, and Compliance department.

Date of Adoption: 07/11/18
Date of Implementation: 01/01/19
Date of Last Review:

Date and Subject of Revision:

No Additional HISTORY.