UNIVERSITY OF OREGON

UO Third-Party Information System Security & Application Integration Assessment Procedure

A. Purpose

This procedure seeks to ensure that third-party information systems or system components that access, process, store or transmit UO data are appropriately managed to protect the confidentiality, integrity and availability of the data. The procedure outlines the steps for conducting assessment of these systems prior to acquisition or renewal by UO units.

B. Definitions

1. **Sensitive Data Environment (SDE)** - computer system or network of systems that directly processes, stores or transmits UO data classified as Sensitive. Please refer to the UO Data Classification Policy (IV.06.02).
2. **SDE Connected System** – all systems that can be used to directly access, modify or change Sensitive data within the SDE.
3. **SSO Integration**.
4. **SOC 2 –** "Service Organization Controls Type 2 is a report on controls by a service organization relevant to security, availability, process integrity, confidentiality or privacy" (American Institute of Certified Public Accountants). An assessment is usually performed by a third-party auditing firm to verify management's assertions of their security and privacy programs, followed by the issuance of the report.
5. **ISO 27001 Certification** – The International Standards Organization 27001 is a well-known and accepted information security management standard for protecting the confidentiality, integrity and availability of data. It has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. Certifications against this standard are acceptable from reputable auditing firms or third-party assessors.
6. **HECVAT –** The Higher Education Cloud Vendor Assessment Tool, and the lightweight version (with a shorter set of questions for review in low-risk situations), was created by the Higher Education Information Security Council (HEISC) Shared Assessments Working Group. Its purpose is to provide a starting point for the assessment of third-party provided cloud services and resources.

C. Scope

All third-party information system or system component (including freeware) that falls within the UO SDE or is deemed an SDE Connected System.

D. Criteria

Acquisition of application systems that meet one or more of the following data usage and integration criteria is required to be reviewed by the Information Security office or its delegates, and custodians of affected systems. Specific criteria:

- The application system falls within the SDE
- The application system is an SDE Connected System

E. Pre-Assessment Procedure

a. Please complete the following *Background Information* (Sponsoring UO Unit, Vendor)

Sponsoring UO Unit		
Unit/Department/Center Name		
Project Sponsor		
Project Sponsor (Phone and email)		
Lead Technical Contact		
Lead Technical Contact (Phone and email)		
Additional UO Contacts ***list any additional administrative contacts or those providing technical support from other units***	**Name**	**Unit**

Service/Software/Application System Description	
Name of Service/Software/Application System	
Short Description	

Hosting Service Provider			
Company Name			
Contacts	**Name**	**Phone**	**Email Address**
Administrative Representative			
Technical Contact			
Reference URL			
Additional Information and Contacts			

b. Please complete the *System Component Management Responsibility Matrix* below (Sponsoring UO Unit, Vendor)

System Component	System Component Management Responsibility (Vendor, Subcontractor, UO, or Shared)	Guidance
1. Physical (Facility) Layer	[Names]	Physical data storage or processing facility (datacenter)
2. Network Infrastructure Layer	[Names]	Network communication devices and infrastructure services, including routers, switches, firewalls, network intrusion detection/protection systems (NIDPS); domain name service (DNS), dynamic host configuration protocol (DHCP), network time protocol (NTP), network authentication systems, Directory services, etc.
3. Operating System & Platform Layer	[Names]	Operating systems and core services management. E.g., Windows OS, Linux, Solaris; file transfer protocol (FTP), secure copy protocol (SCP), etc.
4. Data Layer	[Names]	Data-at-rest or data-in-transit; file systems, database management systems, etc. E.g., MySQL, Oracle, Postgres; unstructured files; NT file system (NTFS), etc.
5. Software & Applications Layer	[Names]	E.g., software as a service (SaaS), platform as a service (PaaS)

c. Please provide detailed answers to the following *Pre-Assessment Questions*

Note: Typically, more information and evidence provided here reduce the need for additional detailed questionnaires.

PA 1.0	Please provide the highest *Classification Level* of the data that will be created, accessed, processed, stored or transmitted by this application system. (See the UO Data Classification Policy (IV.06.02). E.g., data with the highest level of sensitivity includes social security numbers, credit card records, protected health information, certain financial records, etc. Please contact the Information Security Office for assistance in classifying your data. **HIGH RISK DATA**
PA 2.0	Please provide a description of the purpose of the application system/service, including how UO information will be used.
PA 3.0	Please provide an overall architecture of the software/application system showing major subsystems or modules and interconnections (i.e., data flow, application systems architecture, integration points with current UO systems, and network architecture diagrams).
PA 4.0	Please describe your information security program and provide supporting documentation to demonstrate your assertions of security controls. Acceptable documentation includes a SOC 2, ISO 27001 certification, FISMA compliance, Cloud Control Matrix, Attestation of Compliance (AOC), other independent assessments. In the absence of formal attestation documentation, please complete the attached Educause HECVAT.

PA 5.0	Please provide any additional information that you have available outlining security controls for the application systems/service.
PA 6.0	For SaaS-based systems, please describe in detail how the system addresses segregation of duties and provide adequate role-based access controls.
PA 7.0	Please describe how the system supports logging and monitoring ensure that anomalous transactions are detected and investigated for security or privacy incidents. E.g., does the system generate transactional logs showing *who did what when?* Does the system integrate with a SIEM or generate sufficient logs to be ingested into a SIEM for log correlation and data analytics?

F. Assessment Procedure

a. Please review the *Assessment Selection Table* below to determine the type of assessment that should be done and involvement level by applicable units.

Data Classification	System Component Management Responsibility	Acceptable Documentary Evidence	Assessment Type	Responsible	Consult	Inform
Low Risk	Any	Any	Informal	Sponsoring UO Unit		IS/Application & Middleware ISO PCS
Moderate Risk	Vendor Only or UO Only (Valued over $5000)	SOC 2 Type 2, or ISO 27001, or HECVAT Lite	Basic Assessment (Appendix A)	Purchasing & Contracting Services (PCS) or Information Security Office (HECVAT Lite only)	ISO	IS/Application & Middleware
Moderate Risk	Multiple	SOC 2 Type 2, or ISO 27001, or HECVAT Lite	Basic Assessment (Appendix A) Application Architecture & Data Flow Diagram Review (Appendix B)	Information Security Office (ISO)	IS/Application & Middleware	PCS

High Risk	Any	SOC 2 Type 2, or ISO 27001, or HECVAT	Basic Assessment (Appendix A) Application Architecture & Data Flow Diagram Review (Appendix B)	Information Security Office (ISO)	IS/Application & Middleware	PCS

b. **Attribute release.** If the application system is using the InCommon Federation and only requires release of the default set of attributes, no further action is required for this step. Otherwise, the Information Services Application and Middleware team should be consulted.

G. Annual Audit

Annual Audit [future].

UNIVERSITY OF OREGON

Appendix A - Basic Assessment Procedure

1. **SOC 2 or ISO 27001**
    a. **3PAO Legitimacy**. Verify the legitimacy of the 3PAO (third party assessor organization) or Audit Firm.
    b. **Attestation Assessment**. Verify that the attestation document (SOC 2/Type 2 report[1] or ISO 27001 certification):
        - Is current. I.e., the expiration date is within 6 months of the current date;
        - Covers the actual physical datacenter where the application system/service is hosted (see the System Component Responsibility Matrix in the Pre-Assessment section)
    c. **Attestation Evaluation (SOC 2** or **ISO 27001).** Verify that:
        - The **Scope** of the SOC 2 covers "*controls to meet the criteria for the Security and Availability principles set forth in TSP section 100, Trust Services principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy*" for the application system/service under review
        - The **scope** of the ISO 27001 certification covers the application system/service under review
        - The **management asserted controls** in the SOC 2 or ISO 27001 certification address critical requirements, including:
            - Datacenter security
            - Application/Service security
            - Authentication, Authorization, Accounting
            - Business Continuity Planning
            - Network Security (Firewall, NIDPS)
            - Change Management
            - Data Security
            - Database Security
            - Mobile Application
            - Physical Security
            - Policies, Procedures, Processes

[1] Note: SOC 1s and SOC 3s are not acceptable substitutes for a SOC 2.

- System Management and Control
- Vulnerability Scanning
- Incidents Response roles and responsibilities

d. Review the **Testing/Finding/Observations** section of the attestation documentation. Verify that there are **"no exceptions/issues noted"** in the document. Note: if exceptions/issues are present, the assessment should be escalated to ISO for an assessment of associated risks

2. HECVAT or HECVAT Lite Review Procedure

a. Review the REN-ISAC Cloud Broker Index (CBI) to determine if the application system has already been reviewed by an Educause Member Institution and listed on the website. Reviews performed by other Institutes of Higher Education may be leveraged for this review.

b. HECVAT Lite Evaluation

- Verify that the application system/service vendor answers "yes" to all multiple choice questions in major control groups listed below. Then verify that descriptions provided in the open-ended questions are consistent with the multiple choice answers. Note: Any "No" answers or inconsistencies between the multiple choice answers and open-ended description provided by the vendor, requires approval by an Office of Information Security director or the CISO before the assessment can be approved.
  - Application/Service Security
  - Authentication, Authorization, and Auditing
  - Business Continuity Plan
  - Change Management
  - Data
  - Database
  - Datacenter
  - Disaster Recovery plan
  - Firewalls, IDS, IPS, and Networking
  - Physical security
  - Policies, Procedures, and Processes
  - System Management & Configuration

- Vulnerability Scanning

- Review Higher Education Shared Assessment Confirmation section of the HECVAT Lite to determine the vendor's willingness to share the assessment result with the Higher Education community through Educause. If the vendor allows it, successful assessments should be submitted to the REN-ISAC Cloud Broker Index, in accordance with the vendor's shared assessment confirmation, by contacting HECVAT@REN-ISAC.net.

c. HECVAT Evaluation

- Verify that the application system/service vendor answers "yes" to all multiple choice questions in major control groups listed below. Then verify that descriptions provided in the open-ended questions are consistent with the multiple choice answers. Note: Any "No" answers or inconsistencies between the multiple choice answers and open-ended description provided by the vendor, requires approval by an Office of Information Security director or the CISO before the assessment can be approved.
  - Major Control Groups
  - Application/Service Security
  - Authentication, Authorization, and Auditing
  - Business Continuity Plan
  - Change Management
  - Data
  - Database
  - Datacenter
  - Disaster Recovery plan
  - Firewalls, IDS, IPS, and Networking
  - Mobile Applications
  - Physical security
  - Policies, Procedures, and Processes
  - Product Evaluation
  - Quality Assurance
  - System Management & Configuration
  - Vulnerability Scanning

- HIPAA (if the data in scope for the application system/service is considered **protected health information** or PHI)
- PCI DSS (if the data in scope for the application system/service is considered **card holder data** under the Payment Card Data Security Standard)

3. Review Higher Education Shared Assessment Confirmation section of the HECVAT Lite to determine the vendor's willingness to share the assessment result with the Higher Education community through Educause. If the vendor allows it, successful assessments should be submitted to the REN-ISAC Cloud Broker Index, in accordance with the vendor's shared assessment confirmation, by contacting HECVAT@REN-ISAC.net.

UNIVERSITY OF OREGON

Appendix B - Application Architecture & Data Flow Diagram Review

Please review the application system architecture and data flow diagram to ensure that data is appropriately protected throughout its lifecycle, including during:

1. **Creation.** Verify that sensitive data input has appropriate security controls, including trusted input devices, obfuscation controls for sensitive data fields (e.g., SSNs, credit card numbers, passwords, etc.).
2. **Access**. Verify that appropriate role-based controls are in place to ensure that privileged and non-privileged users are provided with access on a need to know basis.
3. **Processing.** Verify that devices that process sensitive information have appropriate security controls including segregation of sensitive processing devices from less secure devices; appropriate input validation controls; limitation of output messages (including error messages) that displays sensitive information.
4. **Storage.** Verify that sensitive data-at-rest is protected using encryption control with appropriate key strengths and key management.
5. **Transmission.** Verify that sensitive data is transmitted in a secure manner including via encrypted files, virtual private networks (VPN), Transaction Layer Security (TLS) or other secure transmission methods.
6. **Backup.** Verify that backup of sensitive data is performed at the same security level as the original data including to physically secure facilities, using secure transport mechanisms, and using appropriate data-at-rest security methods.
7. **Archival.** Verify that sensitive data are appropriately sanitized before archival, or is stored in a secure manner that is similar to that of the original data.
8. **Disposition.** Verify that sensitive data is appropriately disposed such that the data is unrecoverable. Acceptable methods include crypto-shredding, physical destruction of hard drives and other storage devices.