UNIVERSITY OF OREGON

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

A. Purpose

This form seeks to collect information about third-party systems or system components that access, process, store or transmit UO data and serves as input to our assessment process to determine if UO Data is appropriately managed to protect the confidentiality, integrity and availability.

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.

UNIVERSITY OF OREGON

C. Background Information

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 and documentation for the following *Assessment Questions*
Note: Typically, more information and evidence provided here reduces 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?