UCDAVIS
Supply Chain Management

UC Davis – Supply Chain Management
Approval Form for Software and Related Services

This form is to be submitted as an attachment to your KFS request.

Important Message:

UC Information Security Policy No. 3 (IS-3) states the Unit Head is responsible for ensuring the effective management of cyber risks. IS-3 requires a security assessment when the Unit is engaged with a supplier who will be given access to institutional information and/or IT Resources classified at Protection Level 2 or higher (as described on Page 2). UC Davis' Vendor Risk Assessment program is designed to identify risks associated with engaging with a supplier.

Unit Heads should be advised that per IS-3, Units "may bear some or all of UC's direct costs that result from an Information Security Incident under the Unit's area of responsibility if the Information Security Incident resulted from a significant failure of the Unit to comply with this policy." Submission of this form does not absolve the Unit or Unit Head of their responsibility to protect Institutional Information and IT Resources, and managing information security risk in a manner consistent with IS-3. By submitting this form, the Unit Head is accepting the risk of procuring the product/service document in this request and authorizing Procurement to proceed with the transaction.

The Requestor and Unit Information Security Leads (UISL) must complete the following sections:

- General Information
- Data Classification
- Approvals

Executing an Agreement without a Vendor Risk Assessment

Regardless of whether a Vendor Risk Assessment has been performed on a potential service provider, Procurement must still complete the standard Procurement process to ensure that agreements (e.g., contracts) comply with IS-3, when applicable, and with all other required University policies.

GENERAL INFORMATION

*This section should be completed by the **Requestor** or **UISL***

Department:		**Department Head:**	
Business UISL:		**Technical UISL:**	
Service Provider:		**Is this a Service or a Product:**	
Requestor:		**Date:**	
Business Purpose for the product or service requested:			

DATA CLASSIFICATION

*This section should be completed by the **UISL** with assistance from the ISO, if needed. The data classification applies to the specific use described in the business purpose listed above.*

Definitions - Protection/ Availability Levels

P4 – *High*	Institutional Information and related IT Resources whose unauthorized disclosure or modification could result in ***significant fines, penalties, regulatory action, or civil or criminal violations***. Statutory, regulatory and contract obligations are major drivers for this risk level. Other drivers include, but are not limited to, the risk of significant harm or impairment to UC: students, patients, research subjects, employees, guests /program participants, UC reputation related to a breach or compromise, the overall operation of the Location or operation of essential services. (***Statutory***.)
P3 – *Moderate*	Institutional Information and related IT Resources whose unauthorized disclosure or modification could ***result in small to moderate fines, penalties or civil actions***. Institutional Information of which unauthorized use, access, disclosure, acquisition, modification, loss or deletion could result in moderate damage to UC: students, patients, research subjects, employees, community, reputation related to a breach or compromise; could have a moderate impact on the privacy of a group; could result in moderate financial loss; or could require legal action. This classification level also includes lower risk items that, when combined, represent increased risk. (***Proprietary***.)
P2 – *Low*	Institutional Information and related IT Resources that ***may not be specifically protected by statute, regulations or other contractual obligations or mandates, but are generally not intended for public use or access***. In addition, information of which unauthorized use, access, disclosure, acquisition, modification or loss could result in minor damage or small financial loss, or cause minor impact on the privacy of an individual or group. (***Internal***.)
P1 – *Minimal*	***Public information or information intended to be readily obtainable by the public***, but whose integrity is important and for which unauthorized modification is the primary protection concern. IT Resources for which the application of minimum security requirements is sufficient. (***Public***.)

Extracted from IS-3 (10/25/2019)

P-LEVEL:	**P_____**

NOTE: Terms and conditions, including Appendix DS and/or HIPAA BAA where applicable, must be approved by the Supplier / Service Provider prior to any download or engagement. There will be no exception.

APPROVALS

*Approvals from the **Business UISL** and **Technical UISL** are required for Procurement to proceed. By signing this approval, the **Technical UISL** and the **Business UISL** certify that they have conducted the necessary review(s) and authorize UC Davis Procurement to proceed with its contracting process. NOTE: Ink signatures and/or electronic signatures are acceptable.*

ROLE	Signature, Date
Business UISL:	
Technical UISL:	