UCR School of Medicine "Security Intake Form" v.1.1.0

This form is required for any procured service, hardware, or software which may create, store, process, or transmit Institutional Information and/or access IT Resources.

This form is intended to facilitate communication about requirements.

A) Vendor

Company Name: _____ Date: _____

Contact Name: _____ Contact Email: _____

Name and Description of Good(s) and/or Service(s) contemplated:

_____

Is there an existing Agreement to govern and control: _____

Will you agree to the UC T&Cs and UC Appendix-DS [link]:

Important Notes:

- https://security.ucop.edu/resources/for-suppliers.html
- You may be asked to sign the UC Appendix-DS.
- You may be asked to engage in Security Risk Assessment.
- If available, provide an Information Security Plan in alignment with UC Appendix-DS.

Complete questionnaire(s) appropriate to the good and/or service(s) contemplated *(all that apply)*:

I.	On-Prem Software	
1	Describe the Institutional Information typically processed by this solution:	
2	Describe the IT Resource(s) typically involved with this solution:	
3	Do you conduct support services (e.g., warranty / Uniform Commercial Code):	
4	Do you safeguard IT Resources, especially as it relates to network or domain access:	
5	Do you warranty against Illicit Code:	
II.	Software-as-a-Service, "Online Subscription", "eCommerce", AND/OR Software Cloud Connectivity	
1	Describe the Institutional Information accessed (e.g., created, received, collected, etc.):	
2	Do you safeguard Institutional Information and IT Resources:	
3	Will all Institutional Information be stored within the United States:	
4	Will you notify the UC of security incident that may impact Institutional Information:	
5	Do you support external authentication services & 2FA (i.e., SAML2 w/Duo):	
6	Are audit logs available and can they be sent to the customer (i.e., syslog):	
III.	Service Only AND/OR On-Prem Software Technical Support (e.g., warranty / UCC)	
1	Describe the Institutional Information accessed (e.g., created, received, collected, etc.):	
2	Do you have commercially reasonable security mechanisms in place for accessing and safeguarding Institutional Information and IT Resources:	
3	Do employees/affiliates that may access Institutional Information or IT Resources undergo background checks and receive periodic security awareness training:	

Comments or Explanation:

_____