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

A) Vendor

Company: _____ Date: _____

Name: _____ Contact: _____

Name and description of good and/or service:

_____

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

Please complete appropriate questionnaire(s) specific to the good and/or service considered:

☐ I. On-Prem Software

1. Will you/affiliates access (e.g., collect, store, etc.) any Institutional Information?
    a. If yes, please describe the Institutional Information accessed.
    e.g., collect licensing/device info, user logs, etc.
    _____
    b. If yes, do you have commercially reasonable security mechanisms in place to safeguard (& return/dispose of) Institutional Information?
2. Do you have commercially reasonable security mechanisms in place to safeguard IT Resources, especially as it relates to network and/or domain access?
3. Do you warranty against illicit code and take commercially reasonable steps to prevent illicit code?

☐ II. Software-as-a-Service AND/OR On-Prem Software Cloud Connectivity

1. Please describe the Institutional Information accessed.
    e.g., collect user behavior, device info, or location, store student or patient records, etc.
    _____
2. Do you have commercially reasonable security mechanisms in place to safeguard (& return/dispose of) Institutional Information and IT Resources?
    a. Are third-party security assessments performed periodically?
    b. Is sensitive data encrypted in-transport and at-rest?
3. Will all Institutional Information be stored in the United States?
4. Will you notify the UC of any security incident that may impact Institutional Information within 72 hours?
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

1. Will you/affiliates access (e.g., collect, etc.) Institutional Information or IT Resources?
    a. If yes, do you have commercially reasonable security mechanisms in place to safeguard (& return/dispose of) Institutional Information and IT Resources?
2. Do employees/affiliates that may access Institutional Information or IT Resources undergo background checks and receive periodic security awareness training?

Comments or Explanation:

_____

You must provide evidentiary security documentation for Security Review

[e.g., Third-party assessment (e.g., SOC2, ISO 27001 cert, pen test, etc.); HECVAT Lite; HECVAT On-Prem, etc.]

Definitions may be found in "University of California – Systemwide IT Policy Glossary" and "UC Appendix-DS"
https://security.ucop.edu/files/documents/policies/it-policy-glossary.pdf https://www.ucop.edu/procurement-services/policies-forms/legal-forms-current/appendix-ds-8-12-2019.pdf