# Software Procurement Roles and Responsibilities

## Requester

The requester may be a faculty member and/or researcher, student worker, staff member or other workforce member. Below is a summary of the Requester's primary responsibilities in the software procurement process:

*Before starting the software procurement process*

- Understand use cases and confirm that the requested software application meets business requirements.
- Identify the Protection and Availability levels of Institutional Information that will be stored, accessed or transmitted through the Software solution.
- *[Coming soon: Fall 2020] Confirm whether or not the Software solution is already in use at UCI by checking in the approved software list. If so, validate that it is appropriate for the Protection and Availability levels of the desired new use case.*
- *If further help is needed, reach out to the Unit Purchasing Point of Contact for guidance.*

*During the Software procurement process*

- Complete the Software Purchase Questionnaire and send to securityreviews@uci.edu.
- Complete Exhibit 1 of Appendix DS and send to the Software Supplier, along with a request for supporting documentation This generally includes information security and privacy policies, 3rd party assessments of controls – SOC Type II report or similar, and/or a Higher Education Community Vendor Assessment (HECVAT) for cloud solutions.
- Serve as the main point of contact with the Supplier.
- *If further help is needed, reach out to the Unit Purchasing Point of Contact for guidance.*

*After the Software procurement process*

- The role of the Requester following the purchase will vary widely based on the Unit, application and use case. In many cases the original Requester is involved:
    - During the annual Software renewal process.
    - In periodic application risks assessments
    - In evaluating Supplier compliance with SLAs.

## Unit Purchasing Point of Contact

This individual is considered the subject matter expert in the software procurement process for the Unit. They are able to guide the Requester, and in some cases partner with them, in the execution of their responsibilities. The degree to which this takes place differs will differ widely across Units. In most (but not all) instances, the Requester, the Unit Purchasing Point of Contact and the Unit Information Security Lead are different individuals.

*Before starting the Software procurement process*

- Serve as a Unit SME on the Software Procurement Process.
- Stay up to date on changes to the process by attending training sessions and reviewing process web pages.
- Understand the Protection and Availability levels.
- *[Future]* Confirm whether or not the Software solution is already in use at UCI. If so, validate that it is appropriate for the Protection and Availability levels of the desired new use case, and whether the solution has been reviewed from an Accessibility perspective.

*During the Software procurement process*

- Confirm completion of the Software Purchase Questionnaire and (if not already sent) send to securityreviews@uci.edu to start the process.
- Serve as the main point of contact with Procurement and OIT Security.

*After the Software procurement process*

- Provide feedback to OIT and Procurement on process improvement opportunities.

## Procurement Services

UCI Procurement Services establishes procurement and purchasing practices, strategically vets and negotiates contracts for goods and service, including software purchases and renewals for both on premise and cloud solutions.

*Before starting the Software procurement process*

- Educate and support Requesters and Unit Procurement Contacts on the software procurement process, Purchasing documentation (e.g., Standard Purchasing Agreement, Terms & Conditions, Appendix DS, Appendix GDPR, BAA, etc.)
- Understand the Protection and Availability levels.

*During the Software procurement process*

- Serve as the main point of contact for Unit Procurement Contacts.

- Confirm completion of the Software Purchase Questionnaire and (if not already sent) send to securityreviews@uci.edu to start the process.
- Ensure that Software purchases and renewals have gone through the appropriate reviews (e.g., Security, Privacy, PCI, GDPR, HIPAA, Accessibility) prior to finalizing purchase.
- Assisting the Unit Purchasing Point of Contact with drafting agreements, reviewing 3rd party agreements, or edits to Terms and Conditions

*After the Software procurement process*

- Confirm Software solutions added to ServiceNow inventory, including relevant documentation (e.g., Security Risk Review findings, Appendix DS (Data Security), Appendix GDPR, and Purchase Agreement, Supplier Security Documentation), noting exceptions and follow-up items (e.g., at renewal) flagged in Security Risk Review.
- Remind Software application owners to allow >=45 business days before renewals to gather supporting documentation, initiate follow-up reviews (e.g., Security, Privacy, etc.).
- Provide feedback to OIT and Unit Procurement points of contact on process improvement opportunities.

## Unit Information Security Lead

Each Unit at UCI has two Unit Information Security Leads. These individuals are accountable for information security within their Units, and in turn, for = holding 3rd party Suppliers accountable for protecting Institutional Information and Information Resources.

*Before starting the procurement process*

- Serve as a primary Unit SME for information security questions, including those related to Software procurement and post-procurement security and governance.
- Serve as secondary Unit SME on the Software Procurement Process in general.
- Stay up to date on changes to the process by attending training sessions and reviewing process web pages.
- Understand the Protection and Availability levels.

*During the procurement process*

- Initiate, and follow through to completion, the Security Exception Risk Acceptance Process if required (e.g., if a Unit desired to press forward and procure a solution with Security concerns)
- Serve as the main point of contact with the CISO.

*After the procurement process*

- Partner with Software application owners within Units to help hold Software Suppliers accountable for data security and privacy of UCI Institutional Information and Information Resources.
- Update Unit business continuity plans to include contingencies involving the sudden interruption or termination of the Software solution.
- Update EIRIS inventory to include Software solutions that process, store or transmit P3 or P4 data.
    - Ensure completion of bi-annual security risk assessments (i.e., SRAQs) for these solutions either individually, or in partnership with the OIT Security Risk & Compliance team.
- Provide feedback to OIT and Procurement on process improvement opportunities.

## OIT Security Risk and Compliance Team

The OIT Risk & Compliance team performs a significant role in the Software procurement process. While this team's responsibility is to conduct Supplier Security Risk Reviews, there are additional responsibilities.

*Before starting the procurement process*

- Stay up to date on internal (i.e., system-level) and external trends in 3rd party (including Software) risk management through involvement in system-wide working groups, relationships with UCOP Security leadership and participation in system-wide initiatives, events and training.
- Stay up to date on UC policy and practice, emerging risks in 3rd party risk management, and ways to address.
- Create engaging and effective live and virtual training content, web pages, Unit presentations and other informational content to educate stakeholders on Software security principles, including secure procurement.

*During the procurement process*

- Perform Security Risk Reviews and reports findings to Unit Purchasing Point of Contact and Procurement Services.
- When applicable, evaluate Software solutions from a PCI perspective.
- Review and negotiate Appendix DS (Data Security) with the Supplier.
- Partner with Units to execute the Security Exception Risk Acceptance Process if required (e.g., if a Unit desired to press forward and procure a solution with Security concerns).

*After the procurement process*

- Partner with Software application owners within Units to help hold Software Suppliers accountable for data security and privacy of UCI Institutional Information and Information Resources.
- Update Unit business continuity plans to include contingencies involving the sudden interruption or termination of the Software solution.

- Periodically review the EIRIS inventory to ensure newly acquired Software solutions that process, store or transmit P3 or P4 data have been added by Units.
- Support units in their completion of bi-annual security risk assessments (i.e., SRAQs) for these solutions either through a facilitate service, or self-assessment.
- Provide feedback to UCOP and system-wide working groups on improvement opportunities (e.g., Appendix DS).

### Other Stakeholders

Throughout the process, other stakeholders may become play a role in the process based on specific Software solution use cases. Examples of other UCI Campus Units include Privacy, UCI Health, Unit Heads, Legal, Office of Research, Risk, Export Control and more. Representatives from other UC campuses and UCOP may also play a valuable advisory role in the process. Future versions of this document will contain details about each of these additional stakeholders.

## GLOSSARY

Appendix DS (Data Security)
The Data Security Appendix, used system-wide, is required whenever a service provider (including software-as-a-service, or software 'in the cloud' Supplier) will collect, process or maintain Institutional Information or access/provide IT Resources. Most all service providers fall into this category. An Appendix DS is called for in approximately 85% of all software procurements. The main purpose of this document is for the Supplier to demonstrate how they manage cybersecurity and ensure that they notify us if something goes wrong (e.g., a data breach). Appendix DS is a subset of the overall Purchasing Agreement.

EIRIS
EIRIS is a home-grown application that serves as UCI's inventory of protected data across Campus. Each year, all Units on campus confirm that their protected electronic information resources are entered, and current in this system. Currently, EIRIS contains data classified at Protection Level P3 and P4, as well as Critical Infrastructure.

Protection Level (P1, P2, P3, P4)
The UC system uses four levels of data classification, ranging from P1 for publically available data, to P4. UCI has also created a helpful decision tree to help guide workforce members through the process. For specific examples of the types of data, and which Protection Level they are classified in, here is a link to a great guide.

Security Risk Assessment Questionnaire (SRAQ)
The Security Risk Assessment Questionnaire (SRAQ) is UCI's internal tool for assessing risk and compliance in respect to minimum standards and baseline security control requirements. Items in the EIRIS database require a risk assessment every two years. While SRAQs are not part of the procurement process, for more details on how to conduct an SRAQ, please consult this guide.

Unit Information Security Lead (UISL)
Each Unit across campus plays a pivotal role in enabling the UCI Campus Security Program. Unit Security processes are the accountability of Unit Information Security Leads (UISL). Here is a current list of Unit Information Security Leads at UCI. For more details on what this role is accountable for, this role description provides a good overview. This role was formerly referred to as the Information Security Coordinator (ISC).