Software and Cloud Services Acquisition and Renewals Process

This procedure establishes the steps for required risk management practices and due diligence procedures related to the **PURCHASE/ACQUISITION** AND **RENEWALS** of Information Technology systems and applications, including those hosted on-premise and in the cloud.

This process applies to **all system and software acquisitions of all dollar values**[i]. The review process is meant to advise departments on particular threats identified in the potential use of a vendor's product/service offerings, to protect the institution and its data from security breaches and improper use, and to ensure appropriate handling of data at contract termination.

New Purchases/Acquisitions

Step 1

As part of the initiation process for a new software purchase/acquisition, the department must complete the Software and IT Services Form. While completing that form, the department identifies if the software or service is new (vs. a renewal) in the section titled "Purchase Type". For a new purchase, the department must select "Continue to Software Survey."

As part of the Software Survey, several questions will help to identify when/if a security review[ii] is necessary:

- The first question is "Will this application store regulated data"? Regulated data is data that the institution has a legal requirement to protect. The list of major types of data that falls into this category can be found here: http://security.uconn.edu/extended-list-of-confidential-data/. Any system, application, or service that holds any of these data types must have a formal security review.

- The second question largely pertains to cloud-based services. "Does this software/service hold non-public university data or require integrations or data feeds from existing UConn datasets". If the answer is yes, then the system, application or service needs a formal security review.

- The third question addresses the disclosure of personal information in order to foresee and mitigate privacy risks. "Will the University share personal data[iii] with this vendor"? If yes, the requisition will route to Privacy for review and approval.

Once the Software and IT Services Form is completed, the department should submit the requisition using the appropriate Commodity Code. This may include, but is not limited to the following Commodity Codes: 488 (Software, Platform, or Infrastructure as a Service – SaaS, PaaS, IaaS), 489 (Third-Party Application Hosting, 490 (Software Licenses) and/or 491 (Software Maintenance and Support), as appropriate.

Step 2

If the answer to either question 1 or 2 noted in step 1 is "YES", a departmental representative must complete the Security Vendor Review Request Form* located at http://vrm.uconn.edu or by contacting security@uconn.edu[iv].

If the answer to question 3 is yes, the University Privacy Officer will work with the department and vendor contacts to complete a Privacy Impact Assessment (PIA). The PIA is helpful to ensure privacy risks are identified and properly managed and informs the contracting process.

Step 3

Following all necessary dialogue and review processes with the requisitioning Department, Information Security and Privacy approve the requisition in workflow. The final security report and completed PIA will be attached along with any comments indicating approval in HuskyBuy.

Step 4
Upon Procurement's receipt of the requisition, it will be reviewed, prepared, and addressed accordingly. Note that during Procurement's review and prior to completion of the purchase/acquisition, Procurement may include additional business terms for review by Contracting and Compliance, where appropriate.

Renewals

Step 1
As part of the initiation process for renewing a software purchase/acquisition, the department must complete the Software and IT Services Form. While completing that form, the department identifies if the software or service is new (vs. a renewal) in the section titled "Purchase Type".

A renewal may be submitted by selecting any one of the following options: "renewal of maintenance and support", "renewal of license", and "renewal of software, platform or infrastructure as a service", in combination with the following commodity codes

- 488 (Software, Platform, or Infrastructure as a Service – SaaS, PaaS, IaaS),
- 489 (Third Party Application Hosting,
- 490 (Software Licenses) and / or
- 491 (Software Maintenance and Support)

The requisition will then be routed to IT Security for review. Dependent upon the nature of the software or service, additional IT Security or Privacy review may be required upon the advisement of IT Security and Privacy. This may include, but is not be limited to registration of the vendor at http://vrm.uconn.edu, completion of a PIA, etc.

Step 2
Following all necessary dialogue and review processes with the requisitioning Department, Information Security will approve the requisition in workflow. The final security report and completed PIA will be attached along with any comments indicating approval in HuskyBuy.

Step 3
Upon Procurement's receipt of the requisition, it will be reviewed, prepared, and addressed accordingly. Prior to completion of the renewal, this may include additional business terms review and review by Contracting and Compliance where appropriate.

---

[i] Trial or free software must be submitted as a zero-dollar ($0.00) requisition so that it may undergo appropriate contractual, privacy, and security reviews. Free or trial software may still require Procurement Contracting and Compliance to negotiate a contract on behalf of the University, dependent on a variety of factors including but not limited to, institutional risk.

[ii] A security review can be requested of any new software or service at any time by completing the Security Vendor Review Request Form listed in Step 2 or by contacting security@uconn.edu. Completing the security review prior to the purchasing process not only helps to inform decision making but can help improve the acquisition process.

[iii] Personal data is information that is identifiable back to an individual. For example, personal data may include but is not limited to: names, date of birth, education records, social security number, physical and electronic addresses, and medical information. Personal data does not typically include anonymized data in aggregate form.

[iv] Once a Vendor Review Request has been submitted, Information Security will request information from the vendor concerning their security program using the HECVAT Lite standardized questionnaire (for most services). The survey request and any follow-up questions will be handled by Information Security's Vendor Risk Management platform.