

Software Purchasing Process

The Original Software Process



Software is no longer physical



Current Software Procurement Process



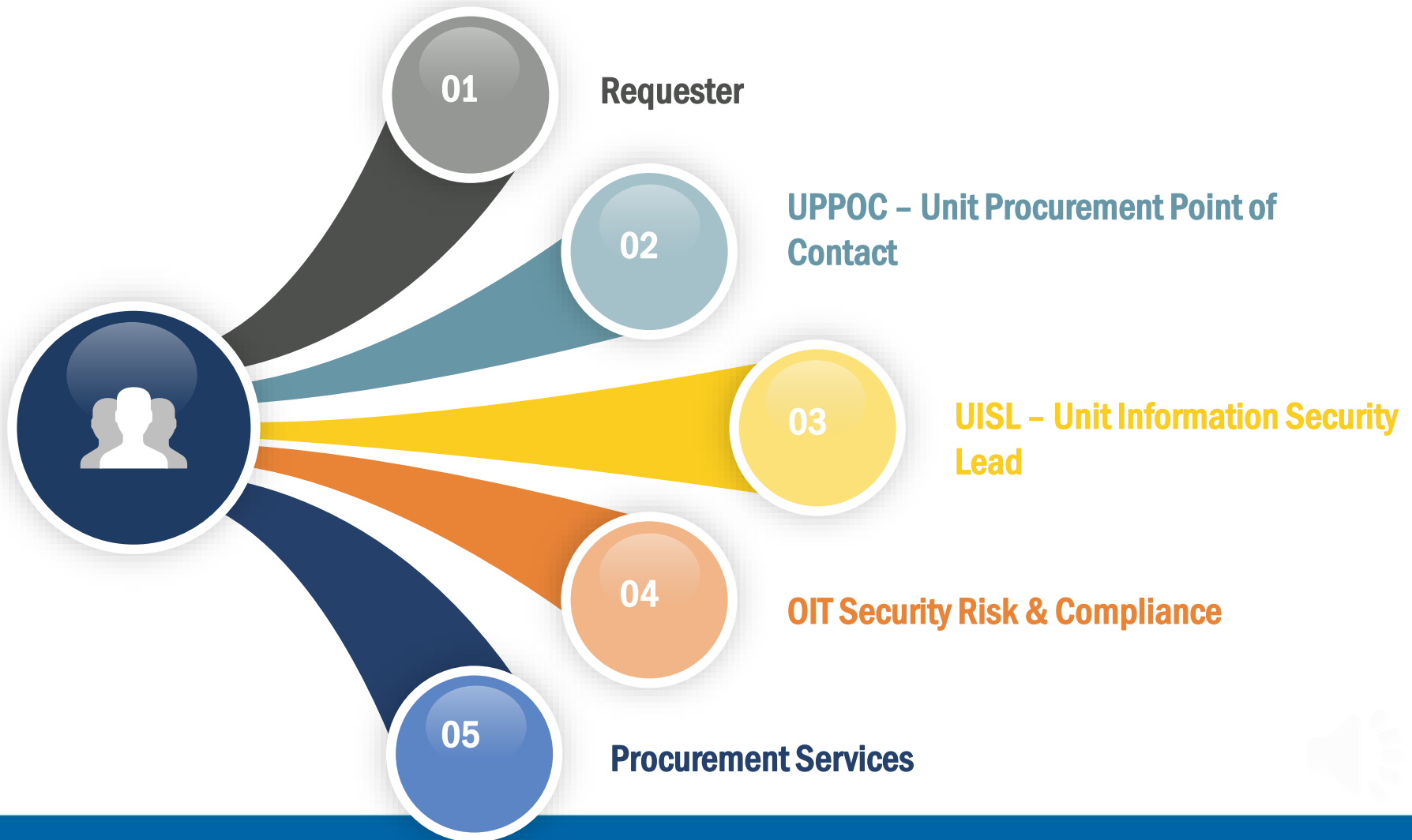
1. End user submits request to dept.
2. Dept. submits KFS requisition or request to PALCard team for approval
3. Procurement verifies if any existing agreements are in place.
4. If no agreement exists, Procurement forwards software questionnaire to dept.
5. Dept. consults with end user and local IT to fill out questionnaire.
6. Dept. submits questionnaire to Procurement for review.

1. Procurement reviews questionnaire and either forwards it to OIT to begin a security review or dept. is given permission to purchase.
2. OIT asks department to request HECVAT, Security Plan, and SOC Type II report from supplier.
3. OIT provides security review assessment and assists departments in completing Appendix DS.
4. Department sends UC Contract templates (UC T&C, Appendix DS, GDPR, BAA) to supplier to review.
5. Supplier provides feedback/edits.
6. Contracts team reviews edits and negotiates with supplier.

1. Agreement is finalized.
2. PO is issued or paid with PALCard.

Additional 2-4 weeks during FY end

Software Procurement Team



Administrative UISLs

Unit	Technical UISL	Administrative UISL
Athletics	<u>Mikel Alustiza</u>	<u>John Hauscarriague</u>
Chancellor's Office	<u>Max Garrick</u>	<u>Tomas Figueroa</u>
Communications	<u>Jim Kreuziger</u>	<u>Karen Imahara</u>
Enrollment Management	<u>Chris Shultz</u>	<u>Patricia Morales</u>
Division of Finance and Administration	<u>Clint Maruki</u>	<u>David Ott</u>
Graduate Division	<u>James Tang</u>	<u>Court Crowther</u>
Health Affairs	<u>Gabriel Gracia</u>	<u>Jim Davis</u>
Human Resources	<u>Christa Chen</u>	<u>Stephen Whelan</u>
Equal Opportunity & Compliance	<u>Max Garrick</u>	<u>May Wang</u>
Office of Information Technology	<u>Josh Drummond</u>	<u>Kian Colestock</u>
Provost/EVC Office	<u>Max Garrick</u>	<u>Tomas Figueroa</u>
Office of Research	<u>Noah Margolis</u>	<u>Sinqui Musto</u>
Student Affairs	<u>Wayne Fields</u>	<u>Edgar Dormitorio</u>
Office of the Vice Provost for Teaching and Learning	<u>Jeremy Thacker</u>	<u>Jennifer Aaron</u>
University Advancement	<u>Ashish Regmi</u>	<u>Lynn Rahn</u>

Find your department's UISL at  security.uci.edu/isc.html



Academic UISLs

School	Technical UISL	Administrative UISL
Claire Trevor School of the Arts	Jason Valdry	Deb Sunday
School of Biological Sciences	Matthew Martinez	Benedicte Shipley
The Paul Merage School of Business	Gary Striano	Tony Hansford
School of Education	Hyuk Kang	Tammy Ho
The Henry Samueli School of Engineering	Dan Melzer	John Romine
School of Humanities	Dwayne Pack	Penny Portillo
Donald Bren School of Information and Computer Science	Bill Cohen	Heike Rau
School of Law	Patty Furukawa	Lisa Rehbaum
School of Physical Sciences	Domingos Begalli	Maria Graziano
School of Social Ecology	Jennifer Lane	Greg Reinhard
School of Social Sciences	Andrew Hill	Becky Avila
Libraries	Adrian Petrisor	Kevin Ruminson
Division of Continuing Education	Erich Delcamp	Bob Rude
College of Health Sciences	Gabriel Gracia	Jim Davis

Find your department's UISL at security.uci.edu/isc.html



OIT Security Team

UCI Campus

- **Josh Drummond**
Chief Information Security Officer
- **April Sather**
Assistant Chief Information Security Officer
- **John Denune**
Security Risk & Compliance Program Manager

UCI Health

- **Gabriel Gracia**
Data Security Manager
- **Steve Chen**
Security Information Protection Architect
- **Uma Rapaka**
IT Security Architect



Procurement Services Team

Procurement/Strategic Sourcing

- **Patrick Ko**
Senior Buyer
- **Sarosh Siganporia**
Strategic Sourcing and Procurement Manager
- **Snehal Bhatt**
Chief Procurement Officer

Contracts

- **Andrew Calderon**
Contracts Manager
- **Laura Moss**
Principal Contracts Analyst
- **Shelia Thomas**
Contracts Analyst



New Software Procurement Process



Old Process (3 - 8 weeks)



New Process (1 day - 4 weeks)

1. Requester completes SW Procurement Questionnaire and submits to UPPOC.
2. UPPOC reviews questionnaire and identifies/completes required Appendices. UPPOC also checks for existing agreements. If no Appendices required, proceed with purchasing.
3. UPPOC completes Appendix DS Exhibit 1 with requester.
4. UPPOC forwards UCI Contract Templates to Supplier for review and requests additional security documents.

5. UPPOC forwards SW Procurement Questionnaire and Supplier documents for Security Review. UPPOC also routes contract documents to Procurement Services and enter a KFS requisition (if applicable). OIT provides security review assessment and reviews/negotiates the Appendix DS. Any other Appendices will be reviewed by their respective parties. OIT will address and resolve any exceptions.
6. In conjunction with OIT, Procurement Services will negotiate contract language with supplier.

7. Agreement is finalized.
8. PO is issued or paid with PALCard.

Additional 2 - 4 weeks during FY end

1. Requester

Completes the Software Procurement Questionnaire and submits to the Unit Procurement Point of Contact.

Name of Software:

Link to Software Website:

Describe the main use(s) of this software and the type of data involved:

Will this software be installed locally at UCI, hosted in the cloud, or a combination of both?

☐ Locally ☐ In the Cloud ☐ Both

Is this a new software purchase, or a renewal?

☐ New ☐ Renewal

SECURITY	Yes	Unsure	No	Notes
Will the Supplier have access to any UC resources (e.g., data, network, systems)?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Could the misuse of this software directly cause harm to life or property ?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Will the software be used to process payments of any kind?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Will this software be used to collect, store, access or transmit data related to any of the following?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
• Data governed by a research contract or grant (e.g., CUI, CDI, CTI, EAR, ITAR)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
• Sensitive identifiable human subject research	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
• Financial information (e.g., student loan/financial aid, accounting payroll)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
• Human resource information (e.g., staff, faculty, student worker personnel)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
• Personally identifiable information (PII) (e.g., full name, email address, date of birth, social security number, home address, telephone number)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
• Protected health information (i.e., subject to HIPAA or Data Use Agreements)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
• Other sensitive medical information (e.g., disability or genetic information)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
• Student education records	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
• Data related to European residents (does not apply to British residents)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
• Other data classified as Protection level 3 (P3) or 4 (P4)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
ACCESSIBILITY	Yes	Unsure	No	Instructions
To the best of your knowledge, is this software, or a previous version of it, already in use on campus?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	IF YES - Stop here. An accessibility review is NOT needed. IF NO/UNSURE - proceed to next question.
Will the software be used by people outside your Unit ?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	IF YES/UNSURE - Stop here. An accessibility review IS needed. Contact it-accessibility-review@uci.edu IF NO - proceed to next question.
Is there an alternative way to perform the task if the software cannot be used due to a disability?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	IF YES - An accessibility review is NOT needed. IF NO/UNSURE - An accessibility review IS needed. Contact it-accessibility-review@uci.edu .

Name of Requester

Email Address

Department/Unit

Date

2. Unit Procurement Point of Contact (UPPOC)

- Reviews the Questionnaire
- Verifies if there are any existing agreements
- In coordination with the UISL, determines if the purchase needs the required Appendices and further Review
- If the purchase is low risk/low dollar, issue PO (referencing UCTC) or pay via PALCard.



3. Requester with UPPOC

Completes Appendix DS Exhibit 1.

University of California

Appendix
Data Security

Exhibit 1 – Institutional Information

1. Protection Level Classification⁴:

- ☐ Protection Level 1
- ☐ Protection Level 2
- ☐ Protection Level 3
- ☐ Protection Level 4

Explanation: [Optional, add detail if needed, may be covered in SOW]

The Protection Level determines the applicable cyber security insurance requirement in the Terms and Conditions.

2. Institutional data element descriptors:

Select all data types that apply:

- A. ☐ Animal Research Data.
- B. ☐ Controlled Technical Information (CTI).
- C. ☐ Controlled Unclassified Information (CUI) – 800-171/NARA.
- D. ☐ Defense Department: Covered Defense Information (CDI).
- E. ☐ Federal Acquisition Regulations (FARS/DFAR) other than CUI.
- F. ☐ GDPR personal data.
- G. ☐ GDPR special data.
- H. ☐ Health data – other identifiable medical data not covered by HIPAA. (Including but not limited to: occupational health, special accommodation, or services qualification, etc.)
- I. ☐ Health Records subject to HIPAA Privacy or Security Rule (PHI).
- J. ☐ Human Subject Research Data.
1. ☐ Identified.
2. ☐ Anonymized.
- K. ☐ Intellectual property (IP), such as patents, copyright, or trade secrets.
- L. ☐ ITAR/EAR-controlled data.
- M. ☐ Payment card data (PCI, PCI DSS).
- N. ☐ Personally identifiable information – PII.
- O. ☐ Student data, whether or not subject to FERPA.
- P. ☐ Other: _____
- Q. ☐ Other: _____

⁴ For reference see: <https://security.ucop.edu/policies/institutional-information-and-it-resource-classification.html>

4. UPPOC

Sends Draft Copies of the UCI Purchasing Agreement, UC Terms and Conditions, and Appendices to the Supplier to review.

AND

Requests the Supplier send to UCI:

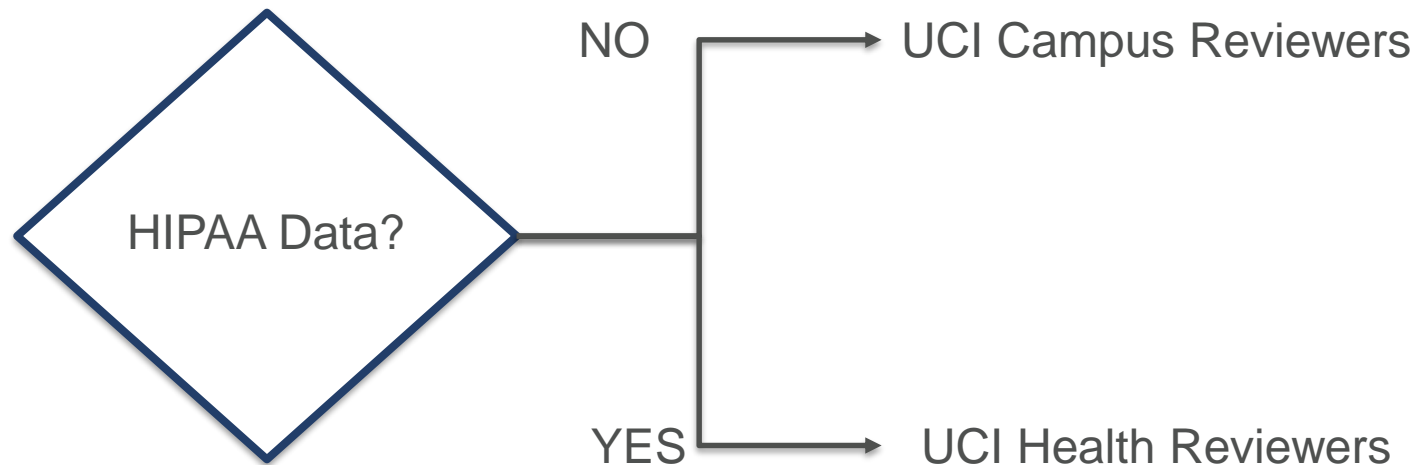
- (a) Information security and privacy policies/plan.
- (b) 3rd party security review (e.g., SOC Type II report)
- (c) HECVAT self-assessment



5. UPPOC

Forwards items to IT Security Team and Procurement Services to initiate the Review Process:

- 1) SW Procurement Questionnaire
- 2) Supplier documents



Submits requisition in KFS

UCI Campus Reviewers

securityreviews@uci.edu

UCI Campus Review Process:

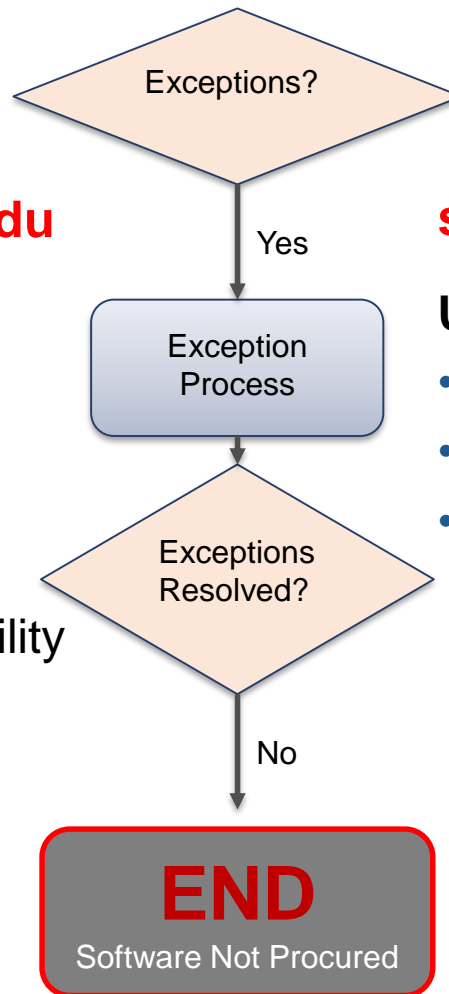
- UCI Campus Security
- UCI Campus Privacy/GDPR
- UCI Campus Accessibility
- UCI PCI

UCI Health Reviewers

secriskassessment@hs.uci.edu

UCIH Review Process:

- UCIH Security
- UCIH Privacy Office/GDPR
- UCIH Accessibility



UCI Campus Reviewers

securityreviews@uci.edu

UCI Campus Review Process:

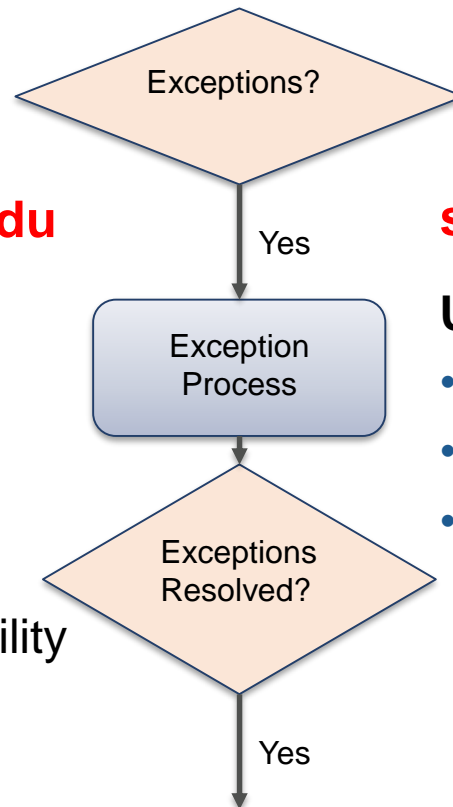
- UCI Campus Security
- UCI Campus Privacy/GDPR
- UCI Campus Accessibility
- UCI PCI

UCI Health Reviewers

secriskassessment@hs.uci.edu

UCIH Review Process:

- UCIH Security
- UCIH Privacy Office/GDPR
- UCIH Accessibility



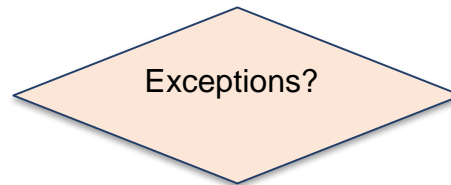
OR

UCI Campus Reviewers

securityreviews@uci.edu

UCI Campus Review Process:

- UCI Campus Security
- UCI Campus Privacy/GDPR
- UCI Campus Accessibility
- UCI PCI



No

UCI Health Reviewers

secriskassessment@hs.uci.edu

UCIH Review Process:

- UCIH Security
- UCIH Privacy Office/GDPR
- UCIH Accessibility



6. Procurement Services

- Reviews/Negotiates any redlines or changes in contract language in parallel with OIT's review process.
- Once the security review and contracts negotiation have concluded, the Contracts Team will finalize the contract (incl. Appendices) and route for signatures.
- Issues Purchase Order or pay via PALCard.
- Adds the software to the University's inventory.

The Rule of Three

Best Practices for End Users/Requesters

1

Submit your requests as early as possible.

2

Consult with your UPPOC first. Be sure to fill out the Software Procurement Questionnaire.

3

NEVER sign any supplier T&C or Agreements on behalf of the University.



The Rule of Three

Best Practices for UPPOC

1

Check for existing agreements. Verify compliance with BUS-43 and PCC.

2

Verify that the Software Procurement Questionnaire is filled out accurately and completely.

3

Allow sufficient time for software review.



Appendix DS

Why Appendix DS?

- To help ensure that UC Institutional Information (the data) and IT Resources (the systems) are kept secure when shared with or access is provided to third-parties.
 - Cloud services
 - Consultants
 - Service/Maintenance Contracts
- Appendix DS applies to:
 - All UC Data (P1 through P4)
 - All purchase amounts from “free” services to multi-million dollar purchases
 - All payment methods including PALCards and purchase orders
- **Does not apply to software only installed and used locally**
 - This line can be a bit blurry...

Components of Appendix DS

- Appendix DS Contract Terms
 - Purpose and Introduction
 - Defined Terms
 - Requirements
- Exhibit 1 - Institutional Information
 - Filled out by the requesting Unit in consultation with Security, Privacy, and other SME's as needed
 - Used to inform the Supplier of the types of data involved in the contract and any legal, regulatory, or contract security requirements
- Exhibit 2 – Supplier's Initial Information Security Plan
 - More on this later...

Appendix DS Requirements in a Nutshell

Suppliers must:

- 3) Agree to protect our data and not sell it or use it for other purposes without our permission
- 4) Have a documented security plan that we can evaluate
- 5) Have some evidence that they are following their own security plan
- 6) Tell us if they make major changes to their security plan, security posture, or have any significant security vulnerabilities in their environment
- 7) Agree to return and/or delete our data when the contract ends
- 8) Tell us (if they are legally allowed to do so) if there are any legal requests for our data
- 9) Tell us if our data is breached, work with us to investigate, and bear notification and other costs as appropriate. A breach can also be grounds for termination.
- 10) Agree not to install backdoors or other illicit code in software or systems
- 11) Agree to perform appropriate background checks on employees that have access to our systems or data

Exhibit 1 in a Nutshell

Three Sections

1. Protection Level

- Determines the applicable cyber security insurance requirements in the Terms and Conditions

2. Institutional Information data element descriptors

- What kind of data is this anyway?

3. Institutional Information Regulation or Contract Requirements

- What are the big legal requirements, regulations, or contract requirements that may/will:
 - Inform the Supplier on how they need to protect the data
 - Determine how UCI negotiates the contracts including Appendix DS and evaluates the Supplier Security Plan
- Document other requirements as appropriate

Exhibit 1, Protection Levels

1. Protection Level Classification⁴:

☐ Protection Level 1

☐ Protection Level 2

☐ Protection Level 3

☐ Protection Level 4

- Refer to Protection Level guidance below. More than one may apply.
- Use the **Classification Decision Tree** to help guide classification decisions
- Provide a short description on what the data is and how it's used

<https://security.uci.edu/security-plan/plan-classification.html>

<https://security.ucop.edu/policies/institutional-information-and-it-resource-classification.html>

Exhibit 1, Data Element Descriptors

2. Institutional Information data element descriptors:

Select all data types that apply:

- A. ☐ Animal Research Data.
- B. ☐ Controlled Technical Information (CTI).
- C. ☐ Controlled Unclassified Information (CUI) – 800-171/NARA.
- D. ☐ Defense Department: Covered Defense Information (CDI).
- E. ☐ Federal Acquisition Regulations (FARS/DFAR) other than CUI.
- F. ☐ GDPR personal data.
- G. ☐ GDPR special data.
- H. ☐ Health data – other identifiable medical data not covered by HIPAA. (Including but not limited to: occupational health, special accommodation, or services qualification, etc.)
- I. ☐ Health Records subject to HIPAA Privacy or Security Rule (PHI).
- J. ☐ Human Subject Research Data.
 - 1. ☐ Identified.
 - 2. ☐ Anonymized.
- K. ☐ Intellectual property (IP), such as patents, copyright, or trade secrets.
- L. ☐ ITAR/EAR-controlled data.
- M. ☐ Payment card data (PCI, PCI DSS).
- N. ☐ Personally identifiable information – PII.
- O. ☐ Student data, whether or not subject to FERPA.

Common Data Elements

- Personally Identifiable Information (PII)
 - Can be P1 through P4
 - Very broad legal definition but can include any detail collected about an individual including names, physical addresses, phone numbers, e-mail address, birthday, physical descriptions, etc.
 - Also includes P4 elements such as SSN, driver's license numbers, credit card numbers, medical information, account names and passwords, etc.
- Health Records subject to HIPAA Privacy or Security Rule (PHI).
 - Protected Health Information (PHI) linked to an individual that is created, collected, transmitted, or maintained by a HIPAA Covered Entity or Business Associate in relation to health care, payments, or healthcare operations
 - **BAA will be required in addition to Appendix DS**
- Health Data – other identifiable medical data not covered by HIPAA
 - Most other medical info including disability services, occupational health, special accommodations, workplace medical documentation, etc.
 - Most medical data used for research falls into this category

Common Data Elements

- Student data, whether or not subject to FERPA
 - More on FERPA later...
- Payment card data (PCI, PCI DSS)
 - All credit card processing activities
 - Especially in cases where UCI is considered the Merchant of Record
 - Additional PCI requirements for all Suppliers involved with card processing
- GDPR Personal Data
 - Very broad category of PII associated with EU residents
- GDPR Special Data
 - Sensitive data on EU residents including racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data concerning a natural person's sex life or sexual orientation

Research Data Elements

- Lots of different types of research data with **additional contract requirements**. Work with your **faculty member** to see if any of these data types are appropriate:
 - Animal Research Data
 - Controlled Unclassified Information (CUI), Defense Department: Covered Defense Information (CDI), and Controlled Technical Information (CTI)
 - Data from the federal government subject to NIST 800-171 requirements
 - Federal Acquisition Regulations (FARS/DFAR) other than CUI
 - Specific federal or DoD regulations
 - Human Subject Research Data
 - Federal protocols usually part of campus IRB review
 - Can be identified or anonymized
 - ITAR/EAR controlled data
 - Export controls relating to sensitive technology and national security
 - Intellectual property (IP), such as patents, copyright, or trade secrets

Exhibit 1, Regulations and Contracts

3. Institutional Information Regulation or Contract Requirements:

Select all regulations or external obligations that apply to inform UC and the Supplier of obligations related to this Appendix:

Privacy (* indicates data security requirements are also present)

- A. ☐ California Confidentiality of Medical Information Act (CMIA) *.
- B. ☐ California Consumer Privacy Act (CCPA).
- C. ☐ California Information Practices Act (IPA).
- D. ☐ European Union General Data Protection Regulation (GDPR)*.
- E. ☐ Family Educational Rights and Privacy Act (FERPA) *.
- F. ☐ Federal Policy for the Protection of Human Subjects (“Common Rule”).
- G. ☐ Genetic Information Nondiscrimination Act (GINA).
- H. ☐ Gramm-Leach-Bliley Act (GLBA) (Student Financial Aid) *.
- I. ☐ Health Insurance Portability and Accountability Act/Health Information Technology for Economic and Clinical Health Act (HIPAA/HITECH) *.
- J. ☐ Substance Abuse and Mental Health Services Administration SAMHSA (CFR 42 Part 2).
- K. ☐ The Fair and Accurate Credit Transaction Act (FACTA).
- L. ☐ The Fair Credit Reporting Act (FCRA).

Exhibit 1, Regulations and Contracts

Data Security

- M. ☐ Chemical Facility Anti-Terrorism Standards (CFATS).
- N. ☐ Defense Federal Acquisition Regulations (DFARS).
- O. ☐ Export Administration Regulations (EAR).
- P. ☐ Federal Acquisition Regulations (FARS).
- Q. ☐ Federal Information Security Modernization Act (FISMA).
- R. ☐ International Traffic in Arms Regulations (ITAR).
- S. ☐ Payment card data (PCI, PCI DSS).
- T. ☐ Toxic Substances Control Act (TSCA).
- U. ☐ Other: _____
- V. ☐ Other: _____
- W. ☐ Other: _____
- X. ☐ Other: _____

Common Laws and Regulations

- California Information Practices Act (IPA)
 - The primary data privacy law for California state government, including UC
 - Protections on how personal information is collected and managed
 - Notification requirements for breach of certain PII
- California Consumer Privacy Act (CCPA)
 - Enhanced privacy protections for California residents
 - Doesn't apply to UC directly but may apply to Suppliers we do business with
- Family Educational Rights and Privacy Act (FERPA)
 - Only applies to data considered part of the official student record
 - Student medical information is covered under FERPA
- European Union General Data Protection Regulation (GDPR)
 - Protects the personal information of EU residents
 - **GDPR Appendix is required in addition to Appendix DS**

Common Laws and Regulations

- HIPAA/HITECH
 - All PHI subject to the HIPAA Privacy and HIPAA Security Rules
 - Generally, does not include data used for research purposes
 - **Requires review by UC Health**
- California Confidentiality of Medical Information Act (CMIA)
 - Basically the California version of HIPAA
- Substance Abuse and Mental Health Services Administration SAMHSA (CFR 42 Part 2)
- Payment Card Data (PCI, PCI DSS)
 - All credit card processing activities
 - **Must be approved by the UCI PCI Committee**
 - **Appropriate Attestation of Compliance (AOC) required**
- Gramm-Leach-Bliley Act (GLBA)
 - Privacy of Student Financial Aid Information
 - May also be subject to NIST 800-171 requirements

Research/Other Regulations

- Federal Policy for the Protection of Human Subjects (“Common Rule”)
- Federal Acquisition Regulations (FARS)
- Defense Federal Acquisition Regulations (DFARS)
- International Traffic in Arms Regulations (ITAR)
- Export Administration Regulations (EAR)
- Federal Information Security Modernization Act (FISMA)
- Chemical Facility Anti-Terrorism Standards (CFATS)
- Toxic Substances Control Act (TSCA)
- Genetic Information Nondiscrimination Act (GINA)
- The Fair and Accurate Credit Transaction Act (FACTA)
- The Fair Credit Reporting Act (FCRA)

Challenges with Appendix DS

- Negotiating Appendix DS terms can be lengthy
 - Large companies often won't negotiate
 - Suppliers with smaller value contracts often don't want to negotiate either
 - Also be wary of Suppliers who accept terms too quickly
- Wide levels of security maturity among Suppliers
 - Many smaller to mid-size companies don't have formal security plans or third-party audits
 - The Higher Education Community Vendor Assessment Tool (HECVAT) can sometimes help bridge the gap
- Security risk assessment depth and final recommendation will depend on:
 - Completeness of the security plan and third-party audits
 - The Protection Level Requirements
 - The specific regulations and contract requirements needed for compliance
 - Security exception process and approvals may be needed for significant gaps

Improving Appendix DS

- One size does **not** fit all
- Small Suppliers have difficulty with formal security plans, background checks, and cyber security insurance
- Low-risk use cases may not need a full security risk assessment
- Future Plans:
 - Develop an Appendix DS Lite for low-risk use cases
 - Develop specific Risk Treatment Plans as a substitute for a formal Supplier security plan in low-risk use cases
 - Provide training and encourage UICL's to do risk assessments for P1-P2 use cases
 - Security Risk and Compliance is exploring the use of a GRC tool to streamline and document Supplier risk assessments
 - Better inventory of pre-approved Suppliers for specific use cases

Risk Driven Security Reviews

Security Review Prior to Purchase	EXEMPT	LIGHT Review	FULL Review	FULL Review – HIPAA Scope
	<ul style="list-style-type: none"> ➤ No security review required prior to purchase. ➤ No Appendix DS required 	<ul style="list-style-type: none"> ➤ Unit-level review and discretion.* ➤ Appendix DS required or comparable Supplier terms* 	<ul style="list-style-type: none"> ➤ Detailed review by OIT Security Risk & Compliance. ➤ Appendix DS required or comparable Supplier terms 	<ul style="list-style-type: none"> ➤ Detailed review by UCI Health Security ➤ Appendix DS required or comparable Supplier terms ➤ Business Associate Agreement (BAA) required
Location + Prot. Level	<ul style="list-style-type: none"> • On premise (i.e., not Cloud) • P1, P2, P3, P4 	<ul style="list-style-type: none"> • Cloud with P1/P2 data 	<ul style="list-style-type: none"> • Cloud with P3/P4 data • Processes payments of any kind 	<ul style="list-style-type: none"> • Cloud with HIPAA Data
Characteristics and Examples	Previously approved for similar use case.	UC directory level information (faculty, staff and students who have not requested a FERPA block)	Supplier will have access to UC P3/P4 resources (network, systems) or institutional information.	Information about health status, provision of health care, payment for health care created or collected by a Covered Entity (or a Business Associate of a Covered Entity), and can be linked to an individual.
	Supplier will not have access to UC resources (data, network, systems)	De-identified research data (in most cases)	Misuse of software could cause harm to life or property	Includes any part of a patient's medical record or payment history.
		Routine business records with P1/P2 data.	Software processes payments of any kind	UCI Health is a covered entity.
		Unpublished research work and intellectual property not classified as P3 or P4.	Financial information	Note: Information related to Student health falls under FERPA, not HIPAA.
		Does not integrate with Canvas	Human resource information	
		Supplier will have access to UC P1/P2 resources (network, systems) or institutional information.	Other sensitive medical information (not HIPAA)	
			Personally identifiable information	
			Canvas integrations	
			Student education records covered by FERPA.	
			Sensitive research	
			Routine business records with P3/P4 data.	

Supplier Privacy Reviews



Learning Objectives

- What is privacy?
- When is a privacy review needed when procuring software?
- Questions to ask suppliers
- Privacy red flags
- Where to direct questions



Privacy Values

- UC respects the privacy of individuals.
- Privacy plays an important role in human dignity and is necessary for an ethical and respectful workplace.

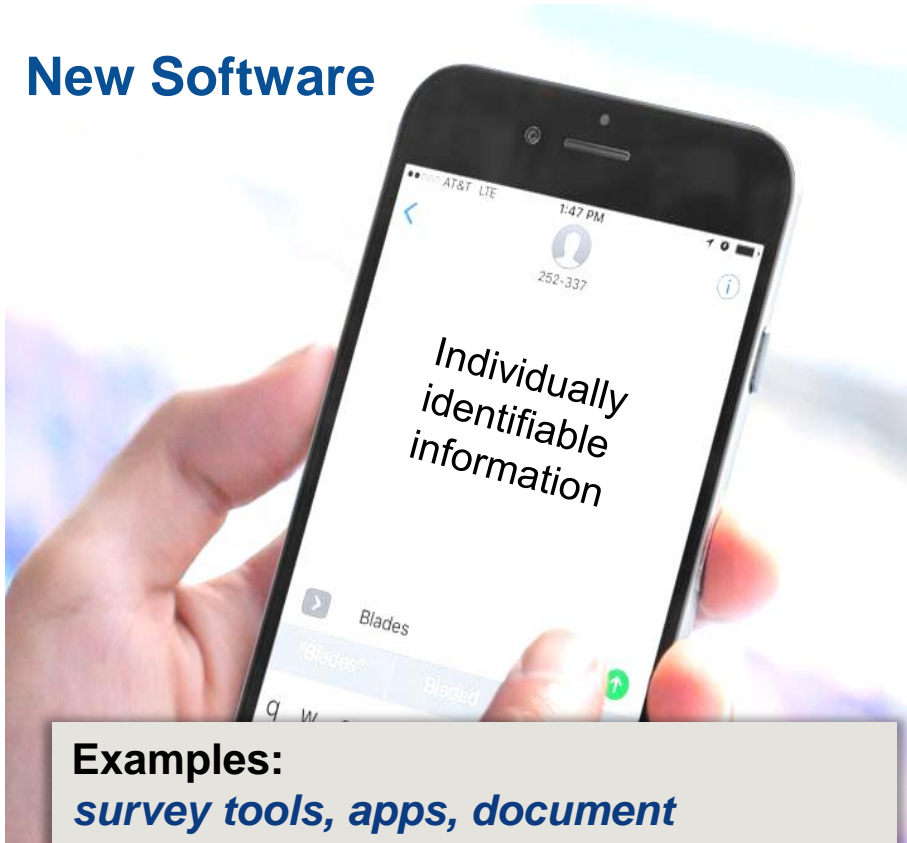
Privacy Principles

- Autonomy Privacy – Individual
- Information Privacy and Security



When is a privacy review needed?

New Software



Examples:

survey tools, apps, document management, cloud storage, cloud backup, eFax, productivity software, event management software, etc.

Renewal or New Uses



Updates to comply with IS-3, GDPR, FERPA, CA and UC Privacy Principles

New uses can require new protections

Software Procurement Questionnaire

Will this software be used to collect, store, access or transmit data related to any of the following?

- | |
|---|
| • Sensitive identifiable human subject research |
| • Financial information (e.g., student loan/financial aid, accounting payroll) |
| • Human resource information (e.g., staff, faculty, student worker personnel) |
| • Personally identifiable information (PII) (e.g., full name, email address, date of birth, social security number, home address, telephone number) |
| • Protected health information (i.e., subject to HIPAA or Data Use Agreements) |
| • Other sensitive medical information (e.g., disability or genetic information) |
| • Student education records |
| • Data related to European residents (does not apply to British residents) |

Privacy in Software Procurement

UCI

Obligations

- Protect privacy rights
- Comply with laws
- Data Classification
- Privacy by Design
- Data Minimization
- Risk Reduction

Questions to Ask Suppliers

- **Where** is UCI institutional information stored?
- **Who** has access?
- What **safeguards** do they use (show us)?
- Will they keep use, **sell or share** our information?
- How will they **notify** UCI if something goes wrong?

Privacy Red Flags



Suppliers who want to **sell our information** to others.



Resistance to **breach notification** requirements.



Suppliers who don't have a **privacy statement or policy**.



Agreements that **exempt suppliers from all liability**.



Privacy Questions?

Thea Bullock, MPA, CCEP

Campus Privacy Official

bullock@uci.edu

Carolyn Cosentino Ponoroff

Asst. Campus Privacy Official

c.cosentino@uci.edu

privacy@uci.edu









Accessible Software Procurement

Why IT Accessibility?









It's the right thing to do!

Disability Variations

	Permanent	Temporary	Situational
Touch	 <p>One arm</p>	 <p>Arm injury</p>	 <p>New parent</p>
See	 <p>Blind</p>	 <p>Cataract</p>	 <p>Distracted driver</p>

Disability Variations

	Permanent	Temporary	Situational
Hear	 Deaf	 Ear infection	 Bartender
Speak	 Non-verbal	 Laryngitis	 Heavy accent

Disability Variations

Permanent

Temporary

Situational

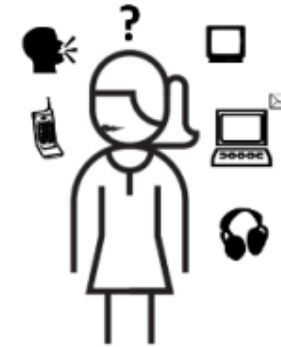
Intellectual



Cognitive disability



Learning, drugs, distress



Interruption, distraction



It's Also the Law – and UC Policy

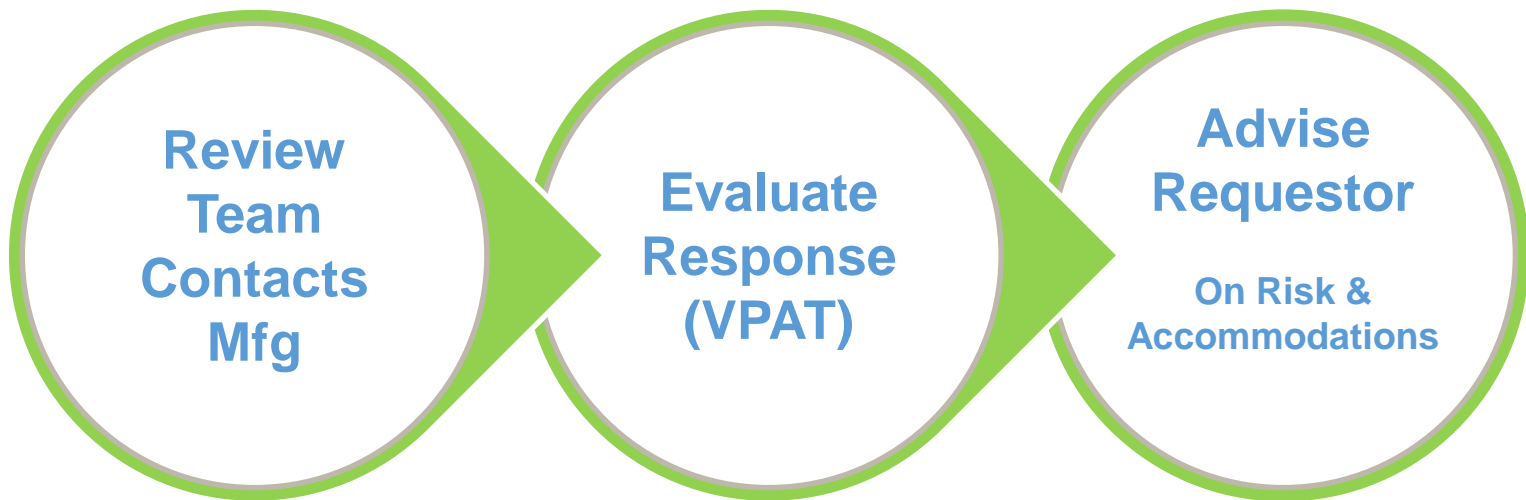
- [Section 508 of the Rehabilitation Act of 1973](#)
- [UC IT Accessibility Policy](#)
- [UCOP Accessible Procurement Guidelines](#)

** All require compliance with WCAG 2.0 guidelines*

3 Questions, with Workflow

ACCESSIBILITY	Yes	Unsure	No	Instructions
To the best of your knowledge, is this software, or a previous version of it, already in use on campus?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	IF YES - Stop here. An accessibility review is NOT needed. IF NO/UNSURE - proceed to next question.
Will the software be used by people outside your Unit ?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	IF YES/UNSURE - Stop here. An accessibility review IS needed. Contact it-accessibility-review@uci.edu IF NO - proceed to next question.
Is there an alternative way to perform the task if the software cannot be used due to a disability?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	IF YES - An accessibility review is NOT needed. IF NO/UNSURE - An accessibility review IS needed. Contact it-accessibility-review@uci.edu .

The Process



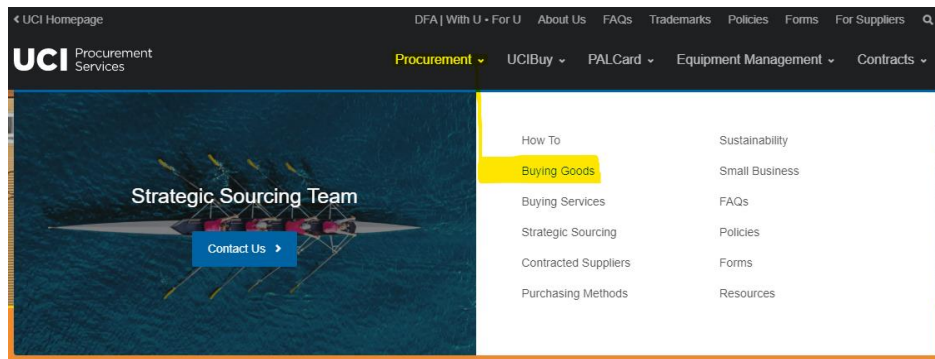


Where do I find ... ?



Questionnaire

- The **software procurement page and questionnaire**
 - On <https://procurement.uci.edu/procurement/software.php>



Home > Procurement > Buying Goods

Using UCIbuy catalogs is the preferred method for purchasing most goods

For purchases greater than \$50,000, contact a Procurement Services Team Member for assistance with benefits and savings negotiations. For purchases using federal funds and/or purchases greater than \$100,000, see Competitive Bidding (RFX) for policies that may apply.



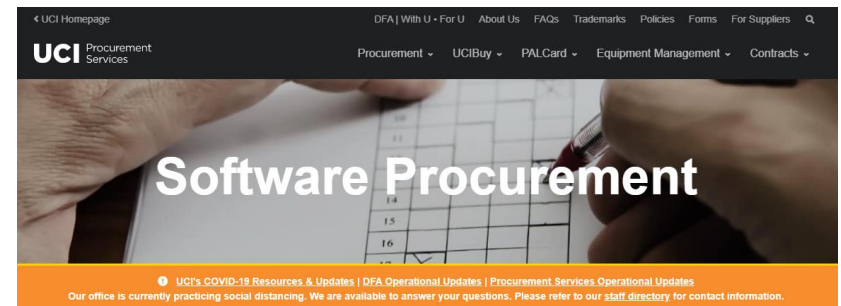
Furniture



Controlled Substances



Software



Home > Procurement > Software Procurement

Make sure you understand what type(s) of software you need (quantity, licenses, compatibility with other equipment, etc.). Since some software purchases are non-returnable/non-refundable, it is very important to ensure that you are purchasing the correct software for your specific needs. There may be an existing university software purchasing agreement that you can utilize for the purchase.

Some of these agreements can be found via the following links:

- Software and Hardware Resources
- Systemwide IT Agreements (XLSX)

Requestor seeking to purchase software that does not have an existing agreement should complete the [Software Procurement Questionnaire \(PDF\)](#). Based on your answers on the questionnaire, your request might require additional review. Please contact your [Unit Procurement Point of Contact \(PDF\)](#) to begin the process. For more information on the software procurement/review process and roles and responsibilities please see the documents below.



Roles and Responsibilities



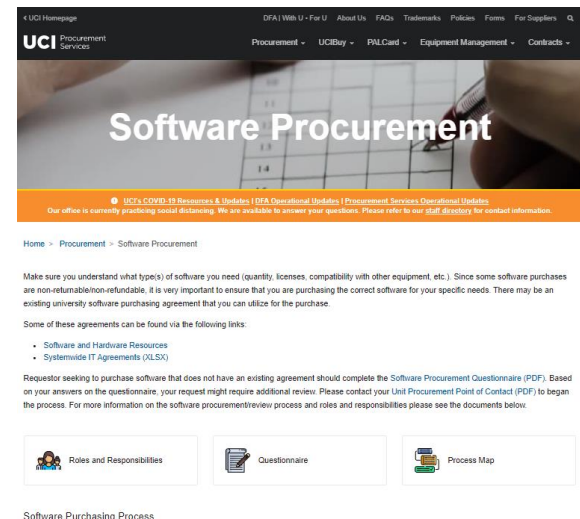
Questionnaire



Process Map

Where do I find ... ?

- This presentation
 - On the [Software Procurement](#) page under the icons.



Where do I find ... ?

- A list of **existing software procurement agreements**
 - An inventory list will be available at the end of 2020
 - Until then...
 - 1st - Check with your Unit Procurement Point of Contact
 - 2nd - Perform a vendor search in KFS for previous software purchase orders
 - 3rd - Contact Procurement Services: procurement@uci.edu



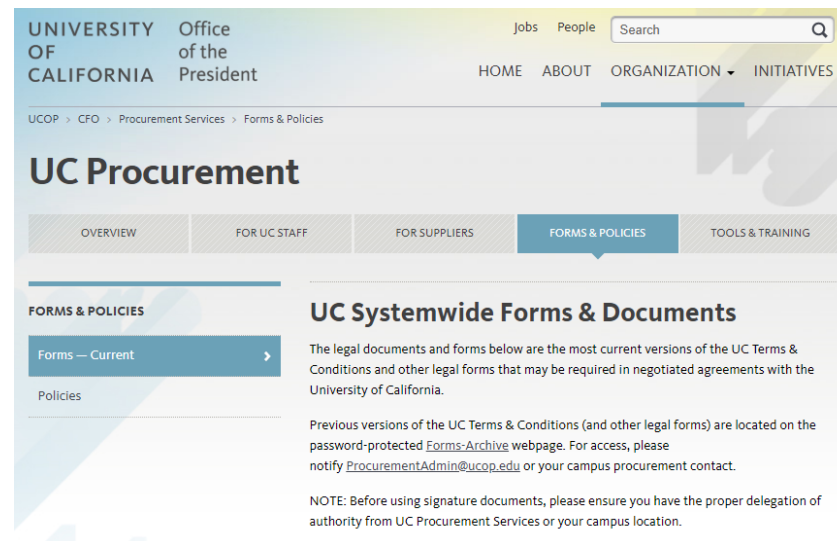
Where do I find ... ?

- Information to help me determine whether to make a software purchase **via PALCard or Requisition**
- For Requestors
 - **Always** start with your UPPOC
- For UPPOC
 - These purchases must be evaluated on a case-by-case basis because it's not the dollar value that matters
 - Sometimes a very small \$ purchase can be toxic and detrimental depending on
 - a) **the type of information** that the supplier will have **access to** **-OR-** what we will **share with** the supplier, and
 - b) how the supplier will **store that information**
 - Contact Procurement Services



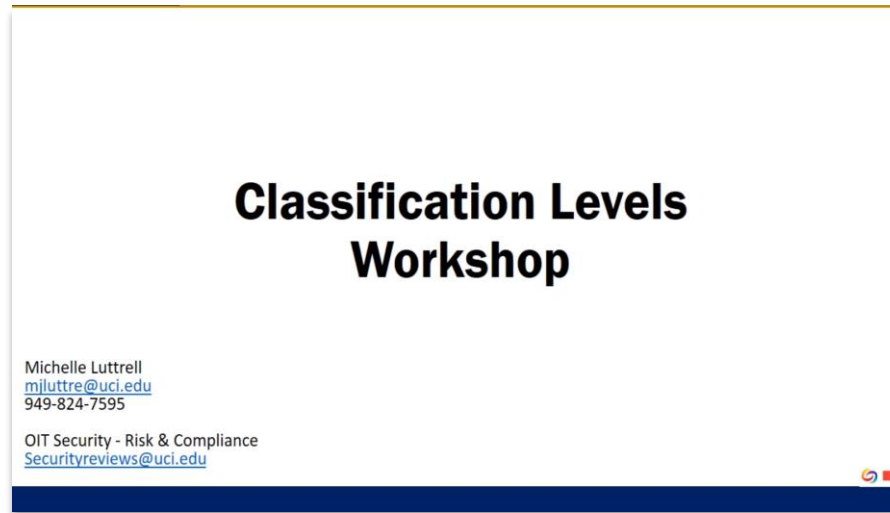
Where do I find ... ?

- The **Appendix DS** and related documents mentioned today
 - <https://www.ucop.edu/procurement-services/policies-forms/index.html>
 - This page has a link to the Appendix DS, with a clickable version of Exhibit 1, and a link to a helpful job aid. It also has links to all the other appendices.



Where do I find ... ?

- The **Classification Levels Workshop** mentioned today
 - [Data Classification Levels Workshop Video](#)
 - [Data Classification Levels Workshop PDF](#)



Where do I find ... ?

- Help on the **software procurement process**

For questions related to...	Contact...
<ul style="list-style-type: none">• UC Terms & Conditions, UC Purchasing Agreement, etc.	<ul style="list-style-type: none">• Unit Procurement Points of Contact and/or Procurement Services
<ul style="list-style-type: none">• Procurement Services	<ul style="list-style-type: none">• procurement@uci.edu
<ul style="list-style-type: none">• Security, the Software Procurement Questionnaire, or Appendix DS**	<ul style="list-style-type: none">• securityreviews@uci.edu
<ul style="list-style-type: none">• Privacy	<ul style="list-style-type: none">• privacy@uci.edu
<ul style="list-style-type: none">• Accessibility	<ul style="list-style-type: none">• it-accessibility-review@uci.edu

*** OIT Security Risk and Compliance is your first point of contact as we roll out this new process. As Units become more familiar, the Unit Information Security Leads (UISL) may choose to become this first point of contact, particularly for software purchases involving P1 & P2 data.*