OR Data Protection Level Assessment

This is the first step in evaluating a software purchase or IT-related vendor services. The outcome of this assessment will determine whether a full campus risk assessment is necessary.

Please answer all of the questions below. Once you complete the assessment, please return the form and the UISL will review the results.

For PI/P2 data, the Unit will review the results and share our findings with you. After review and approval, the purchase may proceed.

If the Data protection Level is identified at P3/P4, you will need to proceed with a Campus Risk Assessment. Please contact your departmental IT support. More information on Data Protection Levels can be found in the UCOP Data Protection Level Classification Guide.

Name of person requesting this assessment
Email of person requesting this assessment
Vendor / Company Name
Vendor Website
Product / Service Name
Summary of business need and proposed use

Does this system contain HUMAN Medical Records, Medical Data, or Human Subjects Research Data?	
☐	Human subject research data with individual identifiers (P4)
☐	Individual identifiable genetic information (P4)
☐	Human protected Health Information (PHI / patient records (P4)
Does this system STORE medical records or medical data which is specifically linked to a patient? (P3/P4)	
○	Yes
○	No
Does this system contain data pertaining to students or instruction?	
☐	Student education records - These records include transcripts and grades, degree information, class schedule, disciplinary records, advising records, and other non-directory information (P3)
☐	Student special services records - These records may contain information needed to provide services or plan accommodations, but for which the student has an expectation of privacy. (P3)
☐	Exams - Questions and answers (P3)
☐	Financial aid information / Student Loans (P4)
☐	Student disability or medical information - Disability information or other medical information collected from students to provide services. (P4)
Does this system contain information about building access systems, IT security plans, or encryption keys? (P3/P4)	
○	Yes
○	No
Does this system contain privileged administrative data? (e.g. financial, payroll, personnel, or legal records)	
☐	Financial, accounting or payroll information (P4)
☐	UC personnel records (P3)
☐	Attorney-Client privileged information (P3)

Does the system contain data protected under Federal regulations. Government contract or IRB designation?	
☐	Controlled Unclassified Information (CUI) (P4)
☐	Covered Technical Information (CTI) or Covered Defense Information (cot) (P4)
☐	Export Controlled Research (ITAR, EAR) Info (P3/P4)
☐	FISMA covered data (P4)
☐	Research information classified as P3 or P4 by IRB, or otherwise required to be stored or processed in a high-security environment (P3/P4)
☐	Data with stringent contractual security requirements (P4)
☐	Government data or data produced that could be classified as P3 or P4
Does the system contain video recordings?	
☐	Security camera recordings (P3)
☐	Body worn video system recordings (P3)
☐	Cameras recording cash or payment card handling areas (P3)
Does this system contain Personally Identifiable Information (PII) or CA Protected Information (PI)? Personally identifiable information (PII) is any data that can be used to identify a specific individual. Social Security numbers, mailing or email address, and phone numbers have most commonly been considered PII, but technology has expanded the scope of PII considerably. It can include an IP address, login IDs, social media posts, or digital images. Geolocation, biometric, and behavioral data can also be classified as PII. Additional Information on PII	
☐	Sensitive Data - An individual's first name (or first initial) and last name in combination with any of the following: Social Security Number, Driver's license number, financial account information such as a credit card number, medical information. (P4)
☐	PII or Pl in large quantity (> 500 records) - Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier IP address, email address, account name (P3)
Does the system contain credit card or cardholder information? (P4)	
○	Yes
○	No

Does the system contain animal research protocols? (P3)	
○	Yes
○	No

If the information or data that the system will store or process was not listed above, please describe the data to be stored or processed.

Is there risk of moderate or significant reputation, financial or other harm or damage to UC Davis if the data is compromised or system becomes unusable?	
○	Yes
○	No

Please select the impact that a theoretical Service Disruption or Loss of Availability would have	
○	A1 - Minimal - Loss of availability may result in minimal impact or minor financial losses. Ex: application installed on personal workstation or laptop. Streaming music &. video
○	A2 - Low - Loss of availability may cause minor losses or inefficiencies. Ex: departmental website. electronic sign board system. general file servers
○	A3 - Moderate - Loss of availability would result in moderate financial losses and/or reduced customer service. Clinical trial management system, public website. ticketing or work management system. time reporting system, tile servers supporting business operations.
○	A4 - Loss of availability would result in major impairment to the overall operation of the University and/or essential services. Ex: Single Sign On (ex: CAS), Email. medical devices, medical records system, financial accounting and payroll systems. core network services.

Is there a risk of fines and/or litigation if the data is compromised or system becomes unusable?	
○	Yes
○	No
Who will have access to the data, and/or service/product?	
☐	Staff/Faculty
☐	Students
☐	Public