Request a Vendor Security Assessment

Please review our service page before submitting your request for a Vendor Security Assessment:

https://security.berkeley.edu/services/vendor-security-assessment-service

Please fill out the form below and press the "Submit" button.

Once submitted, a ticket will be created in ServiceNow and a security analyst from the Information Security Office (ISO) will review your request.

* Indicates required question

1. Email *

2. Buyer's Name *

   You must engage a Buyer to process your purchase.

   Find your Buyer at https://supplychain.berkeley.edu/procurement/find-your-buyer or use the "Buyer Intervention" button in BearBuy when submitting your shopping cart.

3. Buyer's Email *

4. Will the Vendor store, transmit, or handle UC data classified as P3 and/or P4? (Select the highest classification) *

For contracts involving data classified as P1/P2, review and acceptance of security contract language is performed by local Procurement staff using guidance in annotated Appendix DS.

Review the Berkeley Data Classification Standard to classify your data:
https://security.berkeley.edu/data-classification-standard

For questions regarding privacy regulations that may affect classification, contact the Privacy Office (privacyoffice@berkeley.edu).

Mark only one oval.

- ◯ P3
- ◯ P4

5. Will the Vendor have access to UC Berkeley IT Resources classified as P3 and/or P4? *

Examples: Vendor has remote or physical access to UCB IT Resources (devices, APIs, credentials), Vendor consultants with credentials to UCB IT Resources

Mark only one oval.

- ◯ Yes
- ◯ No

6. ATTACH: UCOP Appendix Data Security with the “Exhibit 1 - Institutional Information” section completed. *

The Appendix DS with Exhibit 1 PDF *must be filled out completely* before submitting this request to ISO:

- https://www.ucop.edu/procurement-services/policies-forms/legal-forms-current/appendix-data-security.pdf
- Contact your Buyer for instructions on how to fill out the Exhibit 1 form.
- For questions regarding the applicability of privacy regulations, contact the Privacy Office (privacyoffice@berkeley.edu).

Files submitted:

7. Has your Buyer verified that the Vendor is carrying adequate cybersecurity insurance according to the UC Terms & Conditions' cybersecurity insurance minimums? *

See **Article 9 Section F** for cyber insurance minimums based on data classification in the UC Terms & Conditions: https://www.ucop.edu/procurement-services/policies-forms/index.html

Mark only one oval.

- ◯ Yes
- ◯ No
- ◯ Waiting for evidence of insurance from Vendor

8. Has the Vendor agreed to accept all terms in the Appendix DS without modifications? *

Include the Vendor's proposed Appendix DS modifications ("redlines") in the previous Appendix DS attachment field.

Mark only one oval.

- ◯ Yes
- ◯ No, and the previously attached Appendix DS includes the Vendor's proposed modifications

9. Please select the type of contract *

Mark only one oval.

- ◯ New contract
- ◯ Contract renewal
- ◯ Existing contract with additions or modifications

Unit Information

10. Name of the Unit requesting an assessment *

_____

11. Requester's Name *

The Requester should know the Unit use case for this service and will be the point of contact with the Unit.

12. Requester's Email Address *

Vendor Information

13. Vendor Contact - Name *

Enter the full name of the primary point of contact at the Vendor.

This contact will liaise with Venminder and ISO as needed to provide documentation and information needed to complete the assessment.

14. Vendor Contact - Job Title

If known, enter the job title of the primary point of contact at the Vendor.

15. Vendor Contact - Email Address *

Enter the email address of the primary point of contact at the Vendor.

16. Vendor Contact - Phone Number *

Enter the phone number of the primary point of contact at the Vendor.

17. Name of Vendor *

Enter the name of the Vendor.

- **Example:** If the product/service is Microsoft Windows 10, enter "Microsoft" here.

_____

18. Name of Product/Service *

Enter the name of the product/service. If the name is the same as the Vendor name, just re-enter that.

- **Example:** If the product/service is Microsoft Windows 10, enter "Windows 10" here.

_____

19. Does this product/service have a campus-approved alternative? *

Review the software listed in the following resources:

- BearBUY SHI punch-out, IT Software Catalog https://software.berkeley.edu/software-catalog
- IT Service Catalog https://technology.berkeley.edu/services.

If you are aware of an alternative, but have a specific need for a different product/service, please describe here.

Mark only one oval.

- ◯ No
- ◯ Other: _____

20. Describe the proposed use case(s) of this product/service and the reason why the Vendor needs to have access to UC IT Resources and/or Protected Data. *

Include the following in your description:

- Business need(s) for the Vendor's product/service
- Summarized use case(s) of the Vendor's product/service
- How and why the Vendor will have access to UC IT Resources and/or Protected Data
- Any additional information that can describe the scope of use of the Vendor's product/service

21. Who will use this Vendor product/service? (select ALL that apply) *

Check all that apply.

- [ ] Entire campus
- [ ] Division-wide or by multiple divisions
- [ ] One or more departments within a division
- [ ] One or more academic or division research units
- [ ] General public
- [ ] Students
- [ ] Individual discipline group or subunit within a department
- [ ] Individual research project
- [ ] Trial or pilot
- [ ] Single/one time use case

22. Link to the Vendor’s website describing the product/service (optional)

Protected Data & IT Resources

23. List the key data elements and anticipated Protected Data record count stored, transmitted, or otherwise accessed by the Vendor. *

Examples:

- Names, phone numbers, address, and Social Security Numbers for ~100,000 staff employees
- Residential address, zip code, and identifying health information for ~900 research participants
- Names, email addresses, class names, and class grades for ~40,000 students

24. If the Vendor will have access to UC Berkeley IT Resources classified as P3/P4, describe the nature of the access provided and the IT Resources involved. *

Example: Consultants will be given administrator access to 3 UCB database systems storing P4 data.

25. Exhibit 1 privacy regulations or external obligations *

Check all that apply.

- [ ] Involves access to / collection of personal information
- [ ] FERPA
- [ ] GDPR
- [ ] PIPL
- [ ] HIPAA
- [ ] Other, non-HIPAA medical, genetic, mental health, substance abuse or criminal history information
- [ ] Data Use Agreement includes Privacy requirements
- [ ] None

26. Will the Vendor accept payment card data on behalf of UC? *

NOTE: This includes routing users to third-party payment gateways such as PayPal, Venmo, Shopify, etc.

Example: Vendor's service accepts credit card payments from UC students for yearbook photos

Mark only one oval.

- ◯ Yes *Skip to question 27*
- ◯ No

Skip to question 29

PCI DSS Compliance for Accepting Payment Card Data

Because you indicated the Vendor will accep payment card data on behalf of UC, please complete the following questions related to meeting Payment Card Industry Data Security Standard (PCI DSS) compliance requirements.

NOTE: Requesters are responsible for signing any **Non-Disclosure Agreements (NDA)** if the Vendor requires one to release documentation.

27. Whose Merchant ID will be used to process payments related to this Vendor product/service? *

If you are unsure, work with your Vendor and contact the **UC Berkeley Credit Cards Payment Coordinator (merchantsupport@berkeley.edu)** to determine whose Merchant ID will be used to process payments on UC's behalf. Enter any third-party Merchant ID information if selecting the "Other" option.

Mark only one oval.

- ◯ The Vendor's Merchant ID
- ◯ A UC Berkeley Merchant ID
- ◯ Other: _____

28. ATTACH: PCI DSS compliance documentation *

Please include the Vendor's PCI DSS Self-Assessment Questionnaire (SAQ), Attestation of Compliance (AOC), and any other supporting policies or PCI DSS compliance documentation.

Files submitted:

SOC 2 Type II report for IT Service Providers

SOC 2 Type II applies to any business handling sensitive customer information. It's useful for cloud computing vendors, managed IT services providers, software-as-a-service (SaaS) providers, and data centers. A SOC 2 Type II report examines a service provider's internal controls and systems related to security, availability, processing integrity, confidentiality, and privacy of customer data.

NOTE: Requesters are responsible for signing any **Non-Disclosure Agreements (NDA)** if the Vendor requires one to release documentation.

29. ATTACH: SOC 2 Type II report (if available)

Attach the Vendor's SOC 2 Type II report if available. Providing a Vendor's SOC 2 can greatly streamline your assessment request.

NOTE: Provide the Vendor's ***own*** SOC 2 report, and ***not*** the report of the Vendor's hosting provider (e.g. AWS, Azure, GCP).

Files submitted:

Timeline

30. Describe your timeline for completing the purchase of this product/service. If you have deadlines that will impact funding or other urgency, please specify below.

NOTE: The Vendor may be required to fill out a security questionnaire or provide additional documentation to Venminder. The typical turnaround for an assessment is ***4-6 weeks after Venminder has received all the required documentation***. Please plan accordingly.