
# Software & App Purchasing

## What to Know Before You Buy

**Janelle "Hernandez" Wood,** Financial Services Supervisor, Business Partner Teams 5 & 6
May 8, 2025

UNIVERSITY OF CALIFORNIA
Agriculture and Natural Resources

# Preferred and Easiest Method: AE Punchout Catalogs

- Main Catalogs to Choose From
  - Dell: our preferred software reseller
    - Adobe
    - Finance & Accounting
    - Graphics & Design
  - CDW-G:
    - Communication
    - Reporting & Data Analytics


# Why is AE Punchout the Preferred Method of Purchase?

- No VRA is needed
- No Purchase Agreement is Required
- Digital Software is available to download immediately

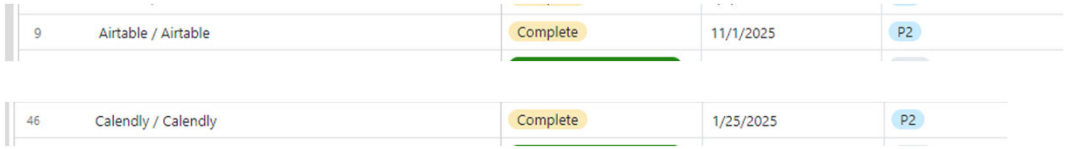
UNIVERSITY OF CALIFORNIA
Agriculture and Natural Resources

# What if Punchout Doesn't Have What I Want?

- Disclaimer: If the following steps are not followed, you will risk an Unauthorized Purchase

# Part 1: Virtual Risk Assessment

- This is processed by our CISO team.
- Request is done via ANR portal
- Depending on the protection level can take up to 8 weeks. (P1-P4)
  - Higher P-level takes longer
- You can check if an Assessment has been completed already AND if it is still valid.




UNIVERSITY OF CALIFORNIA
Agriculture and Natural Resources

# Part 2: UC Davis Procurement Review

- Once VRA is complete.
- Terms & Conditions must be reviewed by UC Davis.
- Can be processed as a PO or No Cost Agreement.
- Turnaround time ~ 3-6 weeks

By using Otter you agree to the Terms of Service and Privacy Policy

**You are not authorized to agree to Terms of Service!**

# Part 2: Back Up Required

- Purchase Request Form
- SRS Form – Signed by Technical UISL
- Copy of completed VRA
- Copy of Terms & Conditions

UCDAVIS
Supply Chain Management

# UC Davis – Supply Chain Management
# Approval Form for Software and Related Services

***This form is to be submitted as an attachment to your Aggie Enterprise request.***

## *Important Message:*

UC Information Security Policy No. 3 (IS-3) states the Unit Head is responsible for ensuring the effective management of cyber risks. IS-3 requires a security assessment when the Unit is engaged with a supplier who will be given access to institutional information and/or IT Resources classified at Protection Level 2 or higher (as described on Page 2). UC Davis' Vendor Risk Assessment program is designed to identify risks associated with engaging with a supplier. A VRA is required for Protection Level 3 or 4 data and should be made available to Procurement upon request.

Per IS-3, Units "may bear some or all of UC's direct costs that result from an Information Security Incident under the Unit's area of responsibility if the Information Security Incident resulted from a significant failure of the Unit to comply with this policy." Submitting this form does not absolve the Unit or Unit Head of their responsibility to protect Institutional Information and IT Resources, and managing information security risk in a manner consistent with IS-3. By submitting this form, the Unit Head is accepting the risk of procuring the product/service documented in this request and authorizing Procurement to proceed with the transaction.

The Requestor and Technical Unit Information Security Lead (UISL) must complete the following sections, regardless of Protection Level:

- General Information
- Data Classification

## APPROVALS

*Approval from the **Technical UISL** is required for Procurement to proceed. By signing this approval, the **Technical UISL** certifies that they have conducted the necessary review(s) and authorize UC Davis Procurement to proceed with its contracting process. NOTE: Ink signatures and/or Adobe E-Signatures are acceptable. Delegate signatures are acceptable, but an email from the Technical UISL or a member of department/unit's leadership designating the individual as the Technical UISL's delegate must be attached to **each** request.*

| ROLE | Signature, Date |
|---|---|
| **Technical UISL:** | Date:___/___/___ |
| **Expiration Date:** | This form is valid through ____/____/____. If P3 data, this form is not to exceed 24 months from the date of the signature above. If P4 data, this form is not to exceed 12 months from date of signature above. |

***Executing an Agreement***

Regardless of whether a Vendor Risk Assessment has been performed on a potential service provider Procurement must still complete the standard Procurement process to ensure that agreements (e.g., contracts) comply with IS-3, when applicable and all other required University policies.

## GENERAL INFORMATION

*This section should be completed by the **Requestor** or **UISL**.*

| | | | |
|---|---|---|---|
| **Department/Entity:** | | | |
| **Technical UISL:** | | | |
| **Service Provider:** | | **Is this a Service or a Product:** | |
| **Requestor:** | | **Date:** | |
| **Business Purpose for requested Product or Service:** | | | |

## DATA CLASSIFICATION

*This section should be completed by the **UISL** with assistance from the ISO, if needed.*

**Definitions - Protection/ Availability Levels**

| | |
|---|---|
| **P4 – *High*** | Institutional Information and related IT Resources whose unauthorized disclosure or modification could result in ***significant fines, penalties, regulatory action, or civil or criminal violations***. Statutory, regulatory and contract obligations are major drivers for this risk level. Other drivers include, but are not limited to, the risk of significant harm or impairment to UC: students, patients, research subjects, employees, guests /program participants, UC reputation related to a breach or compromise, the overall operation of the Location or operation of essential services. (***Statutory***.) |
| **P3 – *Moderate*** | Institutional Information and related IT Resources whose unauthorized disclosure or modification could ***result in small to moderate fines, penalties or civil actions***. Institutional Information of which unauthorized use, access, disclosure, acquisition, modification, loss or deletion could result in moderate damage to UC: students, patients, research subjects, employees, community, reputation related to a breach or compromise; could have a moderate impact on the privacy of a group; could result in moderate financial loss; or could require legal action. This classification level also includes lower risk items that, when combined, represent increased risk. (***Proprietary***.) |
| **P2 – *Low*** | Institutional Information and related IT Resources that ***may not be specifically protected by statute, regulations or other contractual obligations or mandates, but are generally not intended for public use or access***. In addition, information of which unauthorized use, access, disclosure, acquisition, modification or loss could result in minor damage or small financial loss, or cause minor impact on the privacy of an individual or group. (***Internal***.) |
| **P1 – *Minimal*** | ***Public information or information intended to be readily obtainable by the public***, but whose integrity is important and for which unauthorized modification is the primary protection concern. IT Resources for which the application of minimum security requirements is sufficient. (***Public***.) |

*Extracted from IS-3 (10/25/2019)*

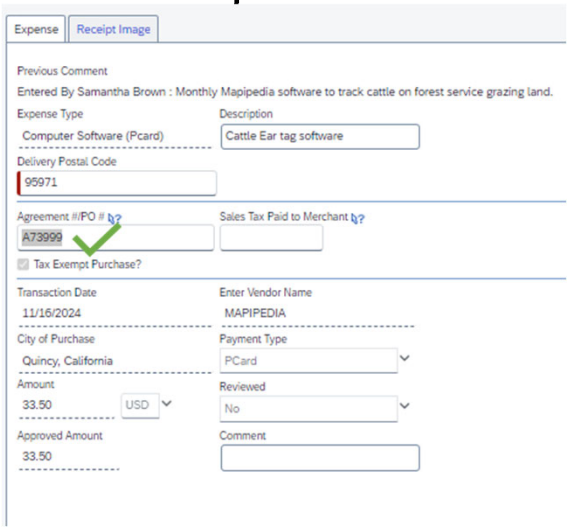
| P-LEVEL: | P_____ |
|---|---|

NOTE: Terms and conditions, including Appendix DS and/or HIPAA BAA where applicable, must be approved by the Supplier / Service Provider prior to any download or engagement. There will be no exception.

UNIVERSITY OF CALIFORNIA
Agriculture and Natural Resources

# Purchasing with a P-Card?

- Still must do VRA ***and*** Procurement Review
  - When reconciling your expense in Aggie Expense you will reference your agreement in the expense line.




UNIVERSITY OF CALIFORNIA
Agriculture and Natural Resources

# Just Downloading an App?

- Still must do VRA ***and*** Procurement Review

# Just renewing the subscription?

- Still MUST have a current VRA ***and*** current PO or Agreement

# Keep ANR Safe!

UNIVERSITY OF CALIFORNIA
Agriculture and Natural Resources

# Questions?

UNIVERSITY OF CALIFORNIA
Agriculture and Natural Resources

# UC Data Security

What is a P-Level

UNIVERSITY OF CALIFORNIA
Agriculture and Natural Resources

# UC Protection Levels (P-Level)

- P1
  - Protection Level 1 (P1)
    - Public Data, intended to be viewed by the public

- Examples
- Blogs
- Public Websites
- Published research
- Press releases
- Marketing materials/advertisements

UNIVERSITY OF CALIFORNIA
Agriculture and Natural Resources

# UC Protection Levels (P-Level)

- Protection Level 2 (P2)
  - Internal data, not specifically protected by regulations
  - Generally not intended for public use
  - Loss results in minor damage or financial loss

- Examples

- Outlook Calendars*
- Internal websites/emails*
- Meeting Notes
- Building plans
- Directory information
- Research using publicly available data
- Email contact lists (less than 500 emails)

*with no P3/P4 data

UNIVERSITY OF CALIFORNIA
Agriculture and Natural Resources

# UC Protection Levels (P-Level)

- Protection Level 3 (P3)
  - Sensitive data, protected by regulations
  - Not intended for public use
  - Loss results in small to moderate fines, penalties or civil actions.
  - Also includes lower risk items that, when combined, represent increased risk

- Examples
- Large external email contact lists (>500)
- Student Records
- Personnel Records
- Security Camera recordings
- Export-controlled research
- Animal research protocols
- IT security-related information

# UC Protection Levels (P-Level)

- Protection Level 4 (P4)
  - Highly sensitive data
  - Not intended for public use
  - Loss results in significant fines, penalties, regulatory action, civil or criminal violations.

- Examples

- Personally Identifiable Information (PII) such as
  - SSN
  - Driver's License #
  - Financial account numbers
  - Biometric or genetic data
  - Health insurance info
- Passwords
- Protected Health Info (PHI or HIPPA Data)
- Credit Card Info (PCI)

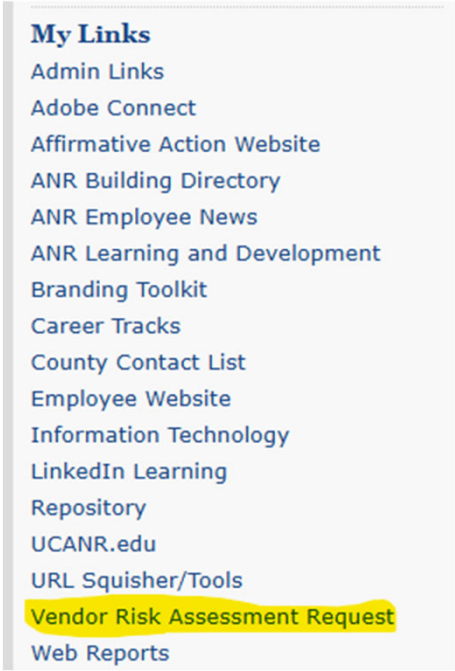
# Vendor Risk Assessments

Process and Advice

UNIVERSITY OF CALIFORNIA
Agriculture and Natural Resources

# UC Requirements & ANR Process

- Suppliers (AKA Vendors) must be assessed for risk
  - What data is the vendor storing?
  - What happens if that data is breached?
  - What is the vendor doing to secure that data?
- Open an **ANR** Risk Assessment
  - Portal – My Links




UNIVERSITY OF CALIFORNIA
Agriculture and Natural Resources

# ANR Process

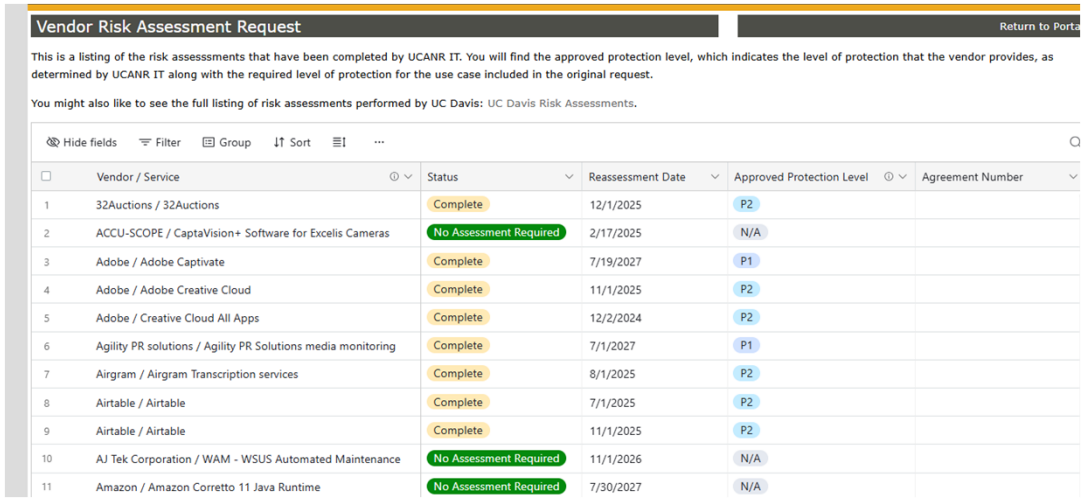
UNIVERSITY OF CALIFORNIA
Agriculture and Natural Resources

- Check the approved vendors:

## Vendor Risk Assessment Initiation Request

NOTE: You can see a full listing of software that has already been risk assessed here: https://ucanr.edu/portal/vra_info.cfm

- List of reviewed vendors



**Vendor Risk Assessment Request** — Return to Porta

This is a listing of the risk assesssments that have been completed by UCANR IT. You will find the approved protection level, which indicates the level of protection that the vendor provides, as determined by UCANR IT along with the required level of protection for the use case included in the original request.

You might also like to see the full listing of risk assessments performed by UC Davis: UC Davis Risk Assessments.

Hide fields | Filter | Group | Sort | ...

| | Vendor / Service | Status | Reassessment Date | Approved Protection Level | Agreement Number |
|---|---|---|---|---|---|
| 1 | 32Auctions / 32Auctions | Complete | 12/1/2025 | P2 | |
| 2 | ACCU-SCOPE / CaptaVision+ Software for Excelis Cameras | No Assessment Required | 2/17/2025 | N/A | |
| 3 | Adobe / Adobe Captivate | Complete | 7/19/2027 | P1 | |
| 4 | Adobe / Adobe Creative Cloud | Complete | 11/1/2025 | P2 | |
| 5 | Adobe / Creative Cloud All Apps | Complete | 12/2/2024 | P2 | |
| 6 | Agility PR solutions / Agility PR Solutions media monitoring | Complete | 7/1/2027 | P1 | |
| 7 | Airgram / Airgram Transcription services | Complete | 8/1/2025 | P2 | |
| 8 | Airtable / Airtable | Complete | 7/1/2025 | P2 | |
| 9 | Airtable / Airtable | Complete | 11/1/2025 | P2 | |
| 10 | AJ Tek Corporation / WAM - WSUS Automated Maintenance | No Assessment Required | 11/1/2026 | N/A | |
| 11 | Amazon / Amazon Corretto 11 Java Runtime | No Assessment Required | 7/30/2027 | N/A | |

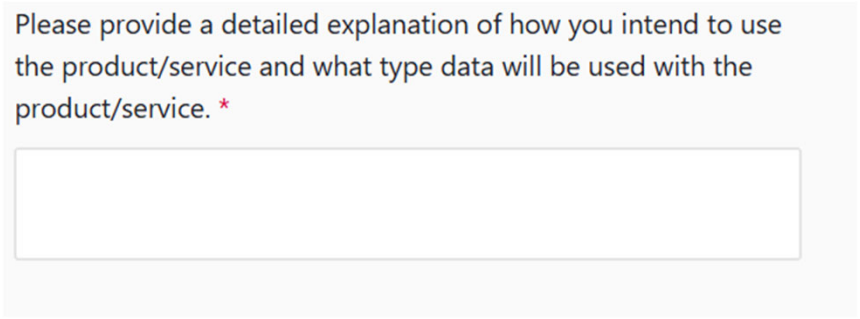
UNIVERSITY OF CALIFORNIA
Agriculture and Natural Resources

# ANR Process

- Vendors already assessed:
  - What Protection Level is the vendor approved for?
  - When does the VRA expire?
  - For P2 or P1
    - Using the same (or lower) protection level of data, no need to open a new VRA, complete the SRS
    - Otherwise open a new VRA request
  - For P3 or P4 – fill out the VRA request
    - IT will share the completed report
  - Unsure?  Open a VRA request

# ANR Process

- Vendor is not assessed or assessment has expired
  - Complete the form, opens a ticket in ServiceNow
  - Be detailed in how you plan to use the application and what data you intend to use with it

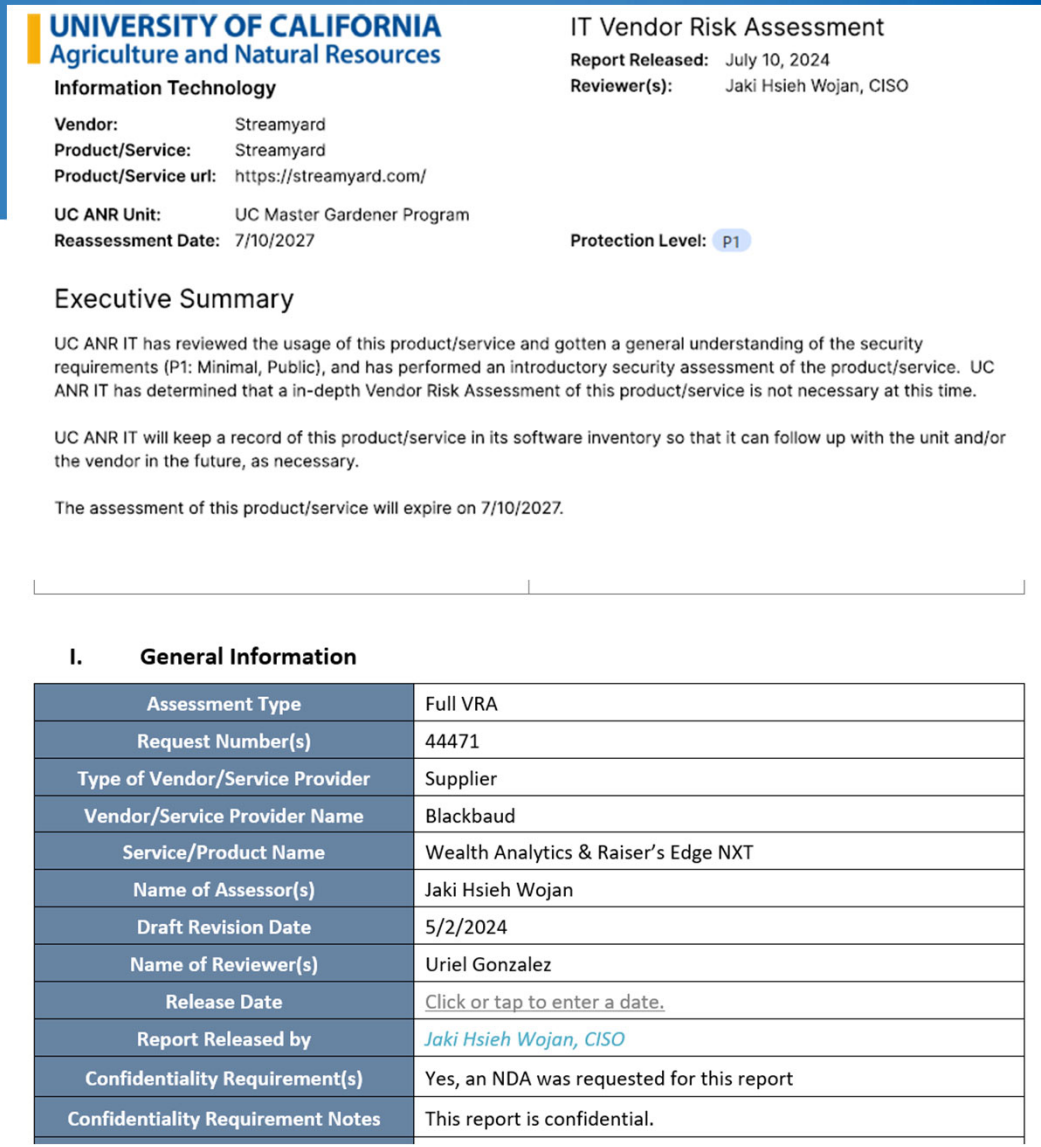



  - For P3 or P4
    - You must include a contact at the vendor.

# ANR Process

- P1 and P2 vendors – VRA lite (Lower Risk)
  - Turn around ~10 to 30 days
  - Verify the data protection level
  - Review privacy policy
  - Standard recommendations

- P3 and P4 – Full VRA report
  - Turn around (30 - 90+ days)
  - Full Security Review
  - SOC 2 Type 2 report
  - ISO certifications
  - HECVAT Questionnaire
  - Venminder partner
  - Requires Appendix-DS
  - What news can we find?



UNIVERSITY OF CALIFORNIA
Agriculture and Natural Resources
Information Technology

IT Vendor Risk Assessment

**Report Released:** July 10, 2024
**Reviewer(s):** Jaki Hsieh Wojan, CISO

**Vendor:** Streamyard
**Product/Service:** Streamyard
**Product/Service url:** https://streamyard.com/

**UC ANR Unit:** UC Master Gardener Program
**Reassessment Date:** 7/10/2027

**Protection Level:** P1

Executive Summary

UC ANR IT has reviewed the usage of this product/service and gotten a general understanding of the security requirements (P1: Minimal, Public), and has performed an introductory security assessment of the product/service. UC ANR IT has determined that a in-depth Vendor Risk Assessment of this product/service is not necessary at this time.

UC ANR IT will keep a record of this product/service in its software inventory so that it can follow up with the unit and/or the vendor in the future, as necessary.

The assessment of this product/service will expire on 7/10/2027.

**I. General Information**

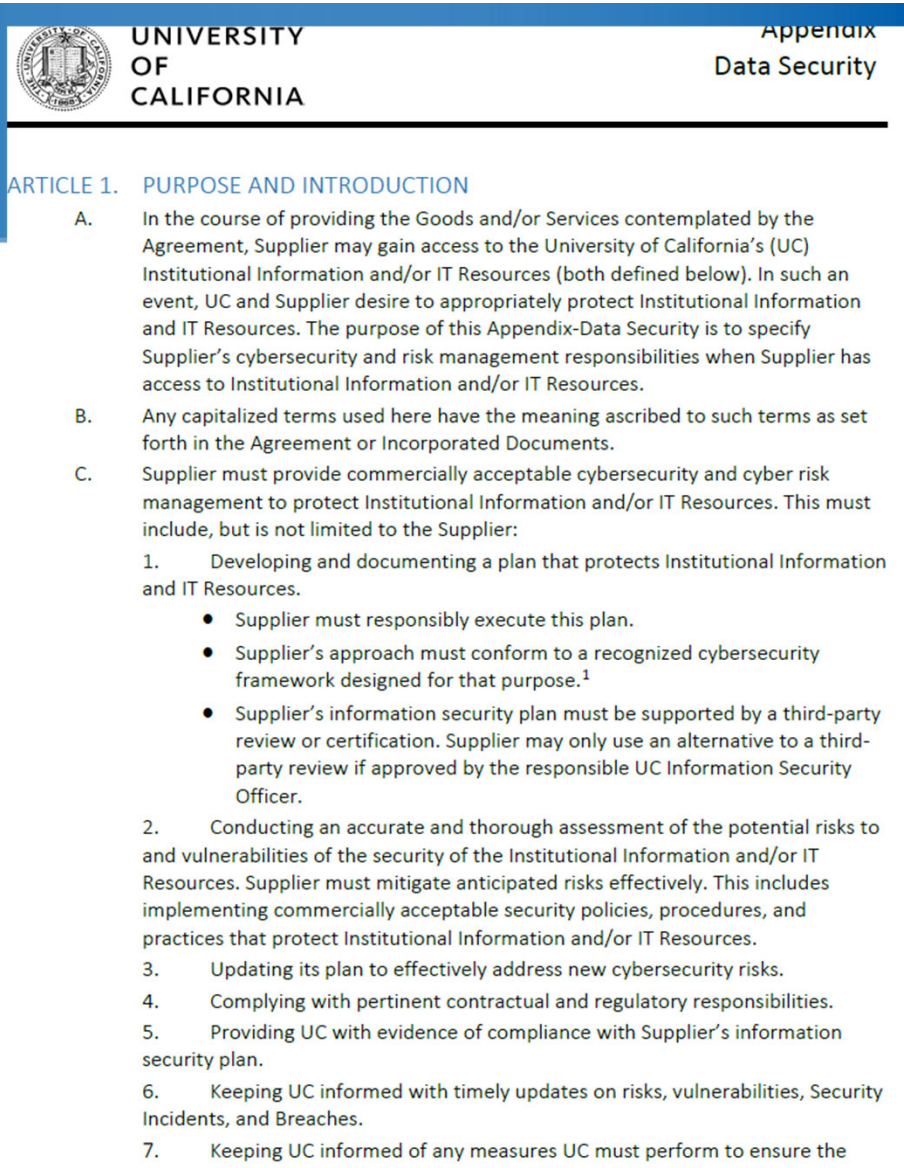
| | |
|---|---|
| Assessment Type | Full VRA |
| Request Number(s) | 44471 |
| Type of Vendor/Service Provider | Supplier |
| Vendor/Service Provider Name | Blackbaud |
| Service/Product Name | Wealth Analytics & Raiser's Edge NXT |
| Name of Assessor(s) | Jaki Hsieh Wojan |
| Draft Revision Date | 5/2/2024 |
| Name of Reviewer(s) | Uriel Gonzalez |
| Release Date | Click or tap to enter a date. |
| Report Released by | *Jaki Hsieh Wojan, CISO* |
| Confidentiality Requirement(s) | Yes, an NDA was requested for this report |
| Confidentiality Requirement Notes | This report is confidential. |

# Appendix Data Security

- Lays out requirements for storing UC's sensitive data
- Some changes can be made by vendor – must be accepted by UC
- Best option:
  - Use approved systemwide vendors

https://www.ucop.edu/procurement-services/for-ucstaff/systemwide-contract-lists/information-technology-agreements.html

  - Use vendors already established in the UC



UNIVERSITY OF CALIFORNIA

Appendix Data Security

ARTICLE 1. PURPOSE AND INTRODUCTION

A. In the course of providing the Goods and/or Services contemplated by the Agreement, Supplier may gain access to the University of California's (UC) Institutional Information and/or IT Resources (both defined below). In such an event, UC and Supplier desire to appropriately protect Institutional Information and IT Resources. The purpose of this Appendix-Data Security is to specify Supplier's cybersecurity and risk management responsibilities when Supplier has access to Institutional Information and/or IT Resources.

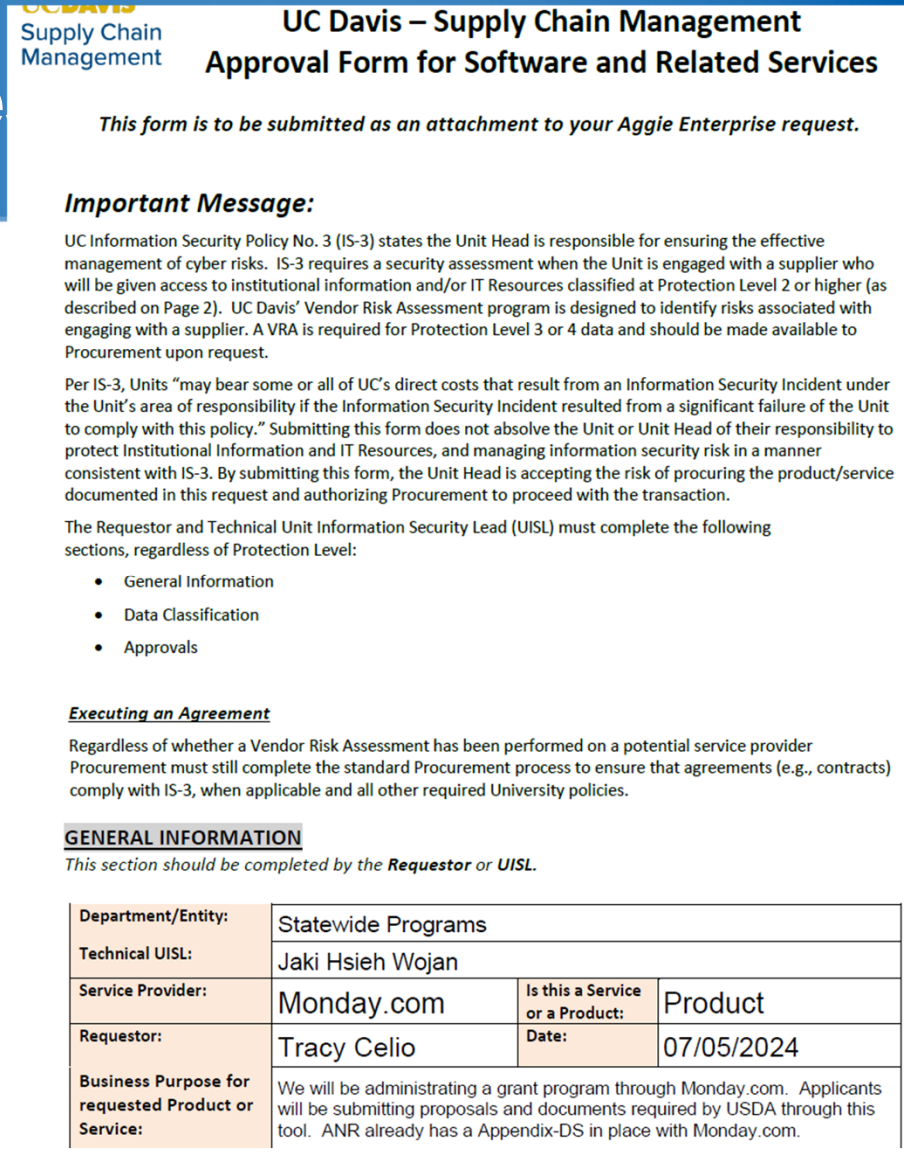
B. Any capitalized terms used here have the meaning ascribed to such terms as set forth in the Agreement or Incorporated Documents.

C. Supplier must provide commercially acceptable cybersecurity and cyber risk management to protect Institutional Information and/or IT Resources. This must include, but is not limited to the Supplier:

1. Developing and documenting a plan that protects Institutional Information and IT Resources.
   - Supplier must responsibly execute this plan.
   - Supplier's approach must conform to a recognized cybersecurity framework designed for that purpose.[1]
   - Supplier's information security plan must be supported by a third-party review or certification. Supplier may only use an alternative to a third-party review if approved by the responsible UC Information Security Officer.
2. Conducting an accurate and thorough assessment of the potential risks to and vulnerabilities of the security of the Institutional Information and/or IT Resources. Supplier must mitigate anticipated risks effectively. This includes implementing commercially acceptable security policies, procedures, and practices that protect Institutional Information and/or IT Resources.
3. Updating its plan to effectively address new cybersecurity risks.
4. Complying with pertinent contractual and regulatory responsibilities.
5. Providing UC with evidence of compliance with Supplier's information security plan.
6. Keeping UC informed with timely updates on risks, vulnerabilities, Security Incidents, and Breaches.
7. Keeping UC informed of any measures UC must perform to ensure the

# Software and Related Service

- Required by UCD
- P2 and P1 – Director can sign as the Technical UISL
- P3 and P4 – CISO will sign as the Technical UISL
- https://supplychain.ucdavis.edu/sites/g/files/dgvnsk2181/files/inline-files/Software_Related_Services_Approval_Form_010824.pdf



Supply Chain Management

**UC Davis – Supply Chain Management**
**Approval Form for Software and Related Services**

***This form is to be submitted as an attachment to your Aggie Enterprise request.***

***Important Message:***

UC Information Security Policy No. 3 (IS-3) states the Unit Head is responsible for ensuring the effective management of cyber risks. IS-3 requires a security assessment when the Unit is engaged with a supplier who will be given access to institutional information and/or IT Resources classified at Protection Level 2 or higher (as described on Page 2). UC Davis' Vendor Risk Assessment program is designed to identify risks associated with engaging with a supplier. A VRA is required for Protection Level 3 or 4 data and should be made available to Procurement upon request.

Per IS-3, Units "may bear some or all of UC's direct costs that result from an Information Security Incident under the Unit's area of responsibility if the Information Security Incident resulted from a significant failure of the Unit to comply with this policy." Submitting this form does not absolve the Unit or Unit Head of their responsibility to protect Institutional Information and IT Resources, and managing information security risk in a manner consistent with IS-3. By submitting this form, the Unit Head is accepting the risk of procuring the product/service documented in this request and authorizing Procurement to proceed with the transaction.

The Requestor and Technical Unit Information Security Lead (UISL) must complete the following sections, regardless of Protection Level:

- General Information
- Data Classification
- Approvals

***Executing an Agreement***

Regardless of whether a Vendor Risk Assessment has been performed on a potential service provider Procurement must still complete the standard Procurement process to ensure that agreements (e.g., contracts) comply with IS-3, when applicable and all other required University policies.

**GENERAL INFORMATION**

*This section should be completed by the **Requestor** or **UISL**.*

| | | | |
|---|---|---|---|
| **Department/Entity:** | Statewide Programs | | |
| **Technical UISL:** | Jaki Hsieh Wojan | | |
| **Service Provider:** | Monday.com | **Is this a Service or a Product:** | Product |
| **Requestor:** | Tracy Celio | **Date:** | 07/05/2024 |
| **Business Purpose for requested Product or Service:** | We will be administrating a grant program through Monday.com. Applicants will be submitting proposals and documents required by USDA through this tool. ANR already has a Appendix-DS in place with Monday.com. | | |