



UCF Vendor Risk Management (VRM) Guide

Why is VRM important?

To minimize the risk to university data, the university needs to take a methodical approach when engaging third party service providers and cloud-based services for data storage, processing or outsourcing of university data. The Vendor Risk Management program (abbreviated VRM) is UCF Infosec's answer to this need.

Does VRM apply to the service I'm looking to acquire?

The VRM process applies to any university department or university business unit considering contracting with a third party service provider for the purposes of storing, transmitting, processing, or collecting university data on our behalf.

In this process, the service-seeking unit submits information about the proposed vendor, solution, and data involved. The Information Security Office (ISO) reviews this package and follows up with the service-seeking unit and/or vendor regarding any questions or concerns. The Information Security Office review results in a formal VRM Assessment report which summarizes what was reviewed, any findings/concerns, and recommendations. The report is reviewed and signed by the appropriate UCF business and data owners, and a signed copy with their signatures must be returned to the Information Security Office.



ServiceNow Ticket Walkthrough

On Behalf Of User

* Open on behalf of this user (Enter user's NID or full name)

▶ More information

UCF Unit Information

* Please select your unit

* Owner (name and @ucf.edu email address)

▶ More information

* Technical Contact (name and @ucf.edu email address)

▶ More information

College/Departmental Security Coordinator/Security Authorizer (name and @ucf.edu email address)

- This section provides the information security office with more information on who's requesting the product and who from the business unit will reach out to the vendor if there's a technical issue. If you're unsure of who this may be for your area, please contact the information security office at infosec@ucf.edu.



☐ Solution / Vendor Information

* Name of Service/Software/System

* Vendor Name

* Vendor Web Page

* Vendor Administrative Representative

* Vendor Technical Contact

Cobblestone Contract ID Number(s)

* Agreement Length

* Short Description / Function

▼ More Information

Please briefly describe what the solution does in a few words. e.g. Customer Relationship Management, Event Management, Classroom Engagement, etc.

* Explain the business need for outsourcing university data processing or handling needs to a third party/vendor. (Please explain how this solutions solves your problem.)

* Does this software use generative or other forms of artificial intelligence that will involve UCF Data?

* Organizational Use?

* Service Type

* Category Type

▼ More information

Which of the available categories does this solution fall into? (Click the magnifying glass to see all available options)


- The solution/vendor information security provides the information security office with basic vendor information that is critical for our review. If you are unsure of how to answer any of the questions, please contact the information security office at infosec@ucf.edu.



[-] SHUD-Q

* Has the vendor completed the Secure Handling of UCF Data Questionnaire?

-- None --

[-] Data Involved 

For definitions and examples of the types of data outlined below (including Highly Restricted/Restricted data), see UCF Policy 4-008: Data Classification and Protection:

* Explain, in detail, what type of data the college and/or department proposes to share (or vendor collects on behalf of UCF) with the third party vendor.

* List any regulations or policies the college and/or department, and in turn the third party vendor must meet (e.g., FERPA, HIPAA, PCI, etc.)

* Does any of the data involved fall under CUI (Controlled Unclassified Information) and/or Export Control requirements?

-- None --

* What is the approximate number of records or individuals' personal data that will be processed and/or shared?

-- None --

- The SHUD-Q (Secure Handling of UCF Data Questionnaire) formerly known as the SHUDA is a document that should be shared with the vendor regardless of the data involved. If there is pushback from the vendor, please contact the information security office.
- Providing the data involved, guides the information security office in their data classification process. If you are unsure or have any questions about what should be listed, please contact the information security office at infosec@ucf.edu.



Data Elements

FERPA/Student

- Academic Standing
- Academic Transcripts
- Class Schedule
- E-mail Address
- Gender
- Grades/GPA
- ISO Number
- Race/Ethnicity
- Religious Preference
- Residency Status
- Social Security Number
- Test Scores
- UCF ID
- UCF NID
- None

Financial

- Bank Account Number
- Billing Information
- Credit Card Expiration
- Credit Card Number
- Credit Card PIN
- Credit History or Score
- Detailed Statement(s)
- Donation Amount(s), Date(s), Codes, etc.
- Donor Details (biographical, educational, etc.)
- Personal Asset(s)
- Personal Expenses or Debt
- Personal Investment Info
- Retirement Information
- Tax Information
- None

- The data elements section also guides the information security office in the data selection process, please try to be as accurate as possible when filling this section out. If there is a data type not listed, please include it in the other data types section. For any questions, please contact the information security office at infosec@ucf.edu.



Implementation Questions

* Who will have access to the system? How will that access be provisioned and deprovisioned?

* Does the vendor integrate with UCF supported Single Sign-On (SSO) solutions such as Active Directory if on-premise or Federation (SAMLv2 or WS_Fed) for cloud applications?

* Will data involved be passed between UCF and the Vendor? If so, how does the data exchange occur? Which on-premise resources or databases will the solution need to connect to (if any)? How often will these data exchanges occur (one time? periodically? Constant?)

* How will the vendor dispose of the data when the contract ends and can they provide a certificate of destruction? Will the vendor hand back the data to UCF after the contract, business arrangement is over, and how useful will that data be?

Attachments

* In order for the Information Security Office to begin a review, some documents must be attached to your submission to ServiceNow. Without these documents, ISO cannot begin a review. To avoid delays, it is up to the UCF unit to collect these documents from the vendor prior to submission.

By checking this box, I confirm that I have attached the "UCF Data Questionnaire (SHUD-Q)" form.

Please see the FAQ item "What Documents do I need to include with my submission?" on <https://infosec.ucf.edu/vrm>.

- The implementation questions provide the information security and data privacy teams with more information on access management and data protection. If you are unsure how to answer a question, please contact the information security office at infosec@ucf.edu.
- For the form to be completed, the completed SHUD-Q from the vendor must be attached to the ticket. If you don't have the document just yet, you can save the ticket to your wish list and ServiceNow will send you reminders on a weekly basis. There may be more documents requested based on data classification, more information about that can be found at [Vendor Risk Management - UCF Information Security](#).

An offline version of the ServiceNow form that you can work with the vendor on, can also be found at [Vendor Risk Management - UCF Information Security](#).