University of Minnesota

Self-Help Guide

Review Process for UMN Software Purchases

This self-help guide outlines the software review process prior to software purchase.

Exploration

Gather Requirements

Understand Your Needs

Use the following checklist to determine your needs before proceeding with a consultation and the rest of the software review process:

- Identify the types of data that will be entered or uploaded, and accessed in this software. The data type should be labeled according to University policy. See: the University Policy Appendix: Data Security Classifications by Type
- Identify potential compliance implications for your data. Depending on how you will use the software, you may be subject to a variety of compliance regulations.
- Identify who will be able to access the data stored and how you will manage access provisioning and deprovisioning.
- Consider the potential need to integrate with University systems; integrations can be challenging and time consuming
- Clarify your timeline

Leverage the Request for Proposal (RFP) Process

Use the RFP Process for Purchases $50,000 and Greater

Standard goods and services totaling $50,000 or greater require a formal competitive bid process called a request for proposal (RFP) that must be performed by Purchasing Services to select a supplier. If your potential purchase meets these requirements, go straight to the RFP process by working with your unit's finance professionals to complete a financial system requisition—requisitions $50,000 and over automatically route to Purchasing Services.

University Policy: Purchasing Goods and Services

Explore Existing University Software

Use Software Directly Supported by IT

It is always advisable to use existing tools and services that have been properly vetted by the University and directly managed and supported by IT professionals.

- Your experience with the software will be more reliable and dependable.
- IT-supported software is vetted for and managed to specific data use cases so your data can be stewarded appropriately.
- Establishing relationships with new vendors can be costly, time consuming, and confusing.
- The continued introduction of new tools and software diffuses the ability of IT to effectively support them.
- IT sprawl leads to inefficiency and greater risk across the University system.

Talk with UMN Community Members

Many solutions are delivered at the University unit level. Reach out to your local IT staff to help identify supported and approved solutions appropriate for your use

case.

Search for Software

Search Atlas
https://atlas.umn.edu/

Some software listed may not be supported or approved—refer to Use Guidance

Search Self Service
/services-technologies/how-tos/self-service-manage-software-university

On University-managed Apple devices

Search Software Center
/services-technologies/how-tos/software-center-manage-software-your

On University-managed Windows devices

Search Technology Help
https://it.umn.edu/

For IT-supported software

Get Help

Request a Consultation

Get Advice can connect you with local IT professionals and subject matter experts.

Submit the Get Advice Request Form
https://tdx.umn.edu/TDClient/31/Portal/Requests/ServiceDet?ID=353

Get Help Using Software

Contact Technology Help
/how-get-technology-help

Vendor Risk Assessment

Understand Security Responsibilities

Review Policies and Resources

Data Security Classification Policy
https://policy.umn.edu/it/dataclassification
FERPA Resources
https://asr.umn.edu/training-and-support/ferpa-resources
Health Information Privacy & Compliance Office
https://healthprivacy.umn.edu/
Payment Card Information Consultation
https://it.umn.edu/services-technologies/resources/payment-card-information-con...

Request a Vendor Risk Assessment (VRA)

What is a Vendor Risk Assessment?

University Information Security (UIS) provides an accurate Vendor Risk Assessment (VRA) to ensure the application is appropriate to support that unit and accurately protect its data according to compliance expectations. UIS will facilitate coordination with data compliance partners like the Health Information Privacy & Compliance Office (HIPCO), the Controller's Office, and Academic Support Resources. UIS will ask for specific information the person/group/unit using the product will need to provide. Things like who will use it and how they will use it, potential data types involved, and how the data is handled and stored. The results of the risk assessment will be shared with the requestor and the local business unit.

Review the Timeline for VRAs

The estimated timeline for the UIS portion of this process is 3–6 weeks, but that can vary as the process depends on back and forth between UIS, the vendor, and the

University contact who can detail how the software will be used.

Initiate the Vendor Risk Assessment Process

Initiate a vendor risk assessment by emailing security@umn.edu.

Contract and Privacy Review

Evaluate Legal Risks

Prepare for Contract Review

University contracts must adhere to established University of Minnesota Regents policies, which are designed to mitigate risk when entering into agreements or other types of business relationships.

Review Regents Policy Related to Contracts
https://ogc.umn.edu/contracts/regents-policies-relating-contracts
Regent's Legal Review of Contracts Policy
https://regents.umn.edu/sites/regents.umn.edu/files/2019-09/policy_legal_review...

Determine if Review is Needed

Review Office of the General Counsel Contract Review Form
https://policy.umn.edu/contracts/standard/ogc-sc515

Review Roles and Responsibilities

Office of the General Counsel

The Office of the General Counsel (OGC) helps business units by reviewing contracts to confirm they comply with applicable laws and regulations. OGC reviews legal terms and addresses legal risk in contracts. All contracts for software, subscriptions,

or IT services may need to be reviewed by the OGC. Even those that are for software that is free.

Local Business Unit

The business unit establishing or modifying a vendor relationship is responsible for and “owns” the relationship with the vendor and the negotiated business terms. The unit is responsible for communicating contract redlines made by OGC with the vendor and determining who has delegated authority to sign an agreement.

Use the University's Supplier Contract Addendum

University’s Supplier Contract Addendum

Using the University’s Supplier Contract addendum can help expedite the process by allowing departments to skip OGC review for lower risk, under $50K agreements when a supplier’s contract is being used. The addendum can not be used without OGC approval if your contract is related to or includes any Private-Restricted or Private-Highly Restricted or other conditions included in the addendum instructions. The local business unit still needs to review the vendor’s contract for business terms as the addendum is only adjusting legal terms to University standards. All business terms need to be negotiated by the department with the supplier.

Access Purchasing Addendum to Supplier's Form
https://policy.umn.edu/contracts/standard/ogc-sc504
Data Security Classification Policy
https://policy.umn.edu/it/dataclassification

Request an OCG Contract Review

Submit Contract Review Form

Submit your Contract Review form via email to ogcpurchasing@umn.edu.

Contract Review Form

https://policy.umn.edu/contracts/standard/ogc-sc515

Learn About Types of Contracts

Quote/Proposal

The Quote or Proposal (may also be called an Order Form) is a document that may be provided by the software provider to the customer before the contract is finalized. It outlines the details of the purchase, including the software titles (e.g., SKU#) being purchased, the quantity of seats if applicable, the price, and the length of the purchase. If customization or configuration is also being purchased from the same supplier, the Quote/Proposal may include a scope of work, deliverables, timelines, and costs. The Quote/Proposal will often link to online Terms of Service. If a Quote/Proposal is not provided, please include a screenshot of the payment screen online that identifies exactly what you will be purchasing.

Master Services Agreement (MSA)

The MSA outlines the overarching terms and conditions that will govern the entire relationship between the software provider and the University. It serves as a framework for future transactions and projects. MSA are more common when a large software provider offers multiple titles which departments may purchase separately. Many contracts will use a TOS/TOU (defined below) in place of an MSA.

Terms of Service (TOS), Terms and Conditions (Ts & Cs), Terms of Use (TOU), Product Specific Terms

The TOS is a legal document that outlines the rules and regulations governing the use of the software by the customer. It covers aspects like user responsibilities, restrictions on use, intellectual property rights, disclaimers, limitations of liability, termination conditions, and any other relevant policies. The TOS may grant the University a license for its users to use the software, or there may be a separate license agreement.

End-User License Agreement (EULA)

EULA is a legal contract between the software provider (licensor) and an individual end-user (licensee). This may be distinct from any license granted to the University as a whole.

Service Level Agreement (SLA)

An SLA outlines the specific performance metrics and standards that the software must meet. It defines factors like uptime, response times, and support availability. SLAs are common in contracts involving software services or cloud-based solutions.

Data Protection and Privacy Addendum (DPA)

This document outlines how personal data will be handled, stored, and protected in compliance with relevant data protection laws.

Statement of Work (SOW)

In some cases, especially for larger software projects that require customization, a Statement of Work may be included. It elaborates on the project's scope, deliverables, timelines, and responsibilities of both parties.