Technology Review: Information Technology and Accessibility Checklist Knowledge Article

UVM has begun performing Technology Reviews prior to any acquisition of technology for use on campus and/or by UVM resources. In scope for this review is the purchase, license, usage or any other contract execution for hardware, software, professional services and/or software maintenance (the “Project”) that commits UVM to terms and conditions regardless of whether it’s a new contract or a renewal. The process is facilitated by the Technology Review Checklist (“Checklist”) and a new Footprints workspace.

The purpose of this Knowledge Article is to accompany the Checklist and provide additional information to assist in filling out the Checklist. The Checklist is designed to assist reviewers in learning about the Project and facilitating the quickest Technology Review possible. Filling out the Checklist thoroughly and providing the requested documents will enable the most expeditious review.

While any UVM employee can initiate a Technology Review, it is critical that the business manager and local IT support are, at a minimum, aware of the request prior to submission. It is recommend that the checklist is completed with assistance from the local IT support and submitted by the Business Manager to ensure all stakeholders are involved.

**Section 1: Vendor Information.**

Please provide information regarding the Vendor.

1. The vendor’s company name should be their company’s legal entity, but may also include their doing business as name (or other name they might be best known by).
2. The product/module name should specify what this particular Project involves, as many vendors sell multiple products.
3. Please provide the best vendor contact name. Generally reviewers will work directly with the UVM requester and allow the requester to maintain the vendor relationship. However, there are times when connecting with the vendor directly may be necessary.

**Section 2: Internal Contact Information**

This section will provide reviewers with information regarding the project requester’s department, their contact information and who can best answer specific questions. This will also allow reviewers to keep the appropriate parties in the loop as the review process continues.

**Section 3: Contract Information**

1. Please provide all contracts and any documents associated with this project. This should include, but is not limited to, the following:
	1. Anything UVM is expected to sign.
		1. Order Forms, Licenses, etc.
	2. Any terms and conditions that govern the relationship between UVM and the vendor.
		1. This may include online terms and conditions, or anything that we must agree to when completing an online ordering process.
	3. In the event there is no contract, please explain the situation.
2. Are there any existing contracts between UVM and the vendor?
	1. Amendments, Renewals, Extensions all build off of existing documents. These earlier documents are important as they provide context to the current document and may need to be modified.
	2. Please provide copies of these documents along with the completed IT Checklist. If you don’t have a copy of the document, please reference that you know it exists and that you don’t have a copy. It is possible that Purchasing has maintained it in their records. You may be asked to request copies from the vendor if UVM has not maintained the documents.
3. Length of Contract Term:
	1. Generally the contract term is defined in the contract and should tell you when the relationship starts and ends. If it isn’t defined, you should discuss this with your department and ultimately with the vendor.
	2. Most technology subscriptions are based on years, please be aware that there is a restriction on how long a contract term may be under UVM guidelines. Purchasing and/or ETS will notify you if this is an issue and work with you to correct any issues.
4. Estimated value over the contract period:
	1. If the contract term is longer than a year (many subscriptions may either be multiple years long or have renewal options), please provide the total amount that will be owed over the life of the contract. If you have specific questions as to how to calculate this amount, please ask.
	2. Sometimes the value of a contract is hard to estimate, for example - if it is based upon usage. Please provide your best guess as to how much you expect to spend over the life of the contract.
5. We like to set the expectation that the review process can take as long as 4 weeks. But we understand that some contracts need to move faster than that. We will take requested timelines into account when we review the Project.

**Section 4: Requested Documents.**

Each of the documents provided by the vendor should be reviewed by you and your team before submitting them for our review. This will allow you to understand what you will be committing to, allow you to ask any questions you might have, and potentially spot concerns/issues.

1. Certificate of Insurance:
	1. This document shows at a glance what levels of insurance the vendor carries.
	2. By adding UVM as a Certificate Holder, UVM will receive notice from the vendor’s insurance company if the vendor’s insurance has changed.
	3. Cyber Risk Insurance:
		1. Risk Management recommends vendors carry at least $5 million in Cyber Risk Insurance in Projects involving any sensitive or protected data.
		2. If the vendor does not carry this level of coverage, then this becomes a business decision for the department.
			1. If the department is willing to accept the risk and proceed with less than $5 million, Risk Management asks that the UVM contact person inform the vendor that UVM is making an exception and that we would expect that the vendor have the higher level of coverage for future engagements with UVM.
2. Voluntary Product Accessibility Template (“VPAT”) and/or Accessibility Conformance Report (“ACR”):
	1. This document will provide insight as to how the Project is designed in relation to accessibility. Vendors create this document to describe how their Project meets standard accessibility guidelines and where it might fall short. Not all vendors will have a VPAT or an ACR.
3. SOC2 Type II Audit Report and other data security related documents:
	1. The SOC2 is an audit conducted by an outside firm to test the vendor’s security posture. Not all vendors will have a SOC2, or they will provide a SOC2 from their cloud service.
	2. Other data security related documents may include, but are not limited to:
		1. Non-SOC2 related audits
		2. Incident Response Plans
		3. Disaster Recovery Plans
		4. Other vendor policies related to data security
4. Other documents:
	1. Depending on the information and documents provided by the vendor, we may request additional documents. One in particular that relates to data security is the Higher Education Cloud Vendor Assessment Tool (“HECVAT”). Not all projects will need the HECVAT, so we will request this document as needed.

**Section 5: Specific Product Information**

Too much information is preferable to too little for all of these sections. Feel free to reference information on the vendor’s website or in materials they’ve provided.

1. Provide a detailed description of what the product is and how it will be used.
2. Describe all pieces of software that will be licensed, provisioned, procured and/or used to satisfy this technology need. Include details about the ongoing application maintenance – who will maintain the software including patches, backups, provisioning – and details about any limitations and/or requirements that exist – are there limited browsers supported or specific Operating systems or specific backend databases, etc.
3. Describe all integrations that are required to make this technology successful at UVM. Include details about who will develop and maintain the integration, whether the integration(s) exist, are provided as part of the solution, or need to be developed, how timely the integration needs to be and the method by which the integration will be written (flat file, API, etc).
4. Describe any/all servers or other hardware that UVM must host in our on premise data centers or otherwise deploy and support in order to make this Technology successful. Include details about the ongoing server maintenance plan – who will maintain the entire stack including Operating System and Application updates, how often will those updates be applied – and details about any servers that are currently provisioned and who in ETS you’ve been working with on this need.
5. Describe who and where this technology will be hosted if it’s somewhere other than on campus. Include all documentation from the hosting provider about their infrastructure and architecture, security policies, backup and recovery, DR, Business continuity, SLAs, etc.
6. If this product/vendor is being selected to meet data security or compliance requirements please provide that information, including information as to what requirement UVM is meeting.
7. Is there a possibility that usage of this technology will expand beyond the scope of this current implementation? If so, how do you foresee this expanding and when might it expand?
	1. The analysis being conducted by ETS and Accessibility focuses on the current (or intended) usage of the Product. However, any additional information about how usage is expected to change in the future will allow for better planning and anticipation of potential future issues. A solid understanding of projected usage could even include that usage will not change based on current projections.
	2. In the event that usage changes over the course of the engagement, please let ETS and Accessibility know that usage has changed if the Project is continued or renewed beyond the initial term.

**Section 6: Information Security**

As a University, UVM is governed by a number of federal statutes. One of these statutes is FERPA, which governs the use of student records. FERPA is intentionally broad, meaning that “student records” encapsulate a number of things that may not intuitively seem to be a student record. As such, we’re looking to learn about all of the data that might be accessed or stored by the Project. We are also looking to understand the scope of the records being accessed or stored, a Project containing information on all students/staff may be a bigger risk than a Project related to some small subset of that population.

* + - 1. Will the Project access, store or process any of the following?
				1. Protected Financial Data:

Including but not limited to:

Social Security Numbers – in general, anytime Social Security Numbers are involved we need to be aware of that.

Credit Card Data

Student Loan Information

* + - * 1. Protected Health Data:

Including but not limited to:

Patient Information

Medical Records

* + - * 1. Protected Student Data:

Includes educational records, or information, maintained by our institution

Education Records under FERPA are defined as:

Records, files, document and other materials which:

Contain information directly related to a student, AND

Are maintained by an educational agency or institution (or by a person acting for such agency or institution).

* + - 1. As such, under this broad definition, most records related to students should be protected – regardless of the level of perceived sensitivity.
		1. This includes 95#s, grades, transcripts, GPAs and academic evaluations, etc.
		2. Directory information, as defined [here](file://C:\Users\rseremet\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\Q772MO0N\Please%20see%20the%20following%20website%20for%20more%20information%20on%20directory%20information%20and%20UVM’s%20policy:%20http:\catalogue.uvm.edu\undergraduate\academicinfo\directoryinformationexclusion\), is generally excluded.
1. Personally Identifiable Information

This information may be similar to the directory information described above, but may have an added level of protection warranted under Privacy laws, such as the European Union’s GDPR.

* + - 1. Will the Project integrate into UVM’s Single Sign On solution such that NetID and network passwords are used for authentication? If so, describe the technical details (to include options to use Shibboleth, CAS, SAML, In Common, etc). Has this been discussed with ETS?
			2. Are there any other data security related concerns for this vendor?

**Section 7: Accessibility Information**

The goal of the Accessibility review is to understand who will be using the Project and how it will be used. Many in the UVM community face some form of accessibility issues, and having an understanding as to what challenges may be faced by users can go a long way in remediating concerns.

1. Please describe the group of people (students, faculty or staff) who will be using this Project with as much detail as possible. If the Project is narrowly focused in any way (just a specific department, just a certain research project, etc.) please make that clear. The more information we have related to the universe of people using a Project the more specific our review can be. We would also like to understand how many people will be using the technology, even if it is just an estimate.
2. Please let us know if the potential users of the Project include the public, generally via the internet. The scope and severity of a Project being inaccessible tends to rise as more people have access.
3. Barriers to the Project can come in many forms. Please try to describe any potential issues you might see, as it relates to (this list is not exhaustive):
	1. The inability of a person to use a mouse. Some users will only use a keyboard when using a computer, can they still effectively use the Project technology?
	2. A person who is either blind or has low-vision.
	3. A Deaf person, or someone who is hard of hearing.
4. Along with these questions, please let us know if you have had any accessibility discussions with the vendor and what information they have provided you. This can include providing a copy of the vendor’s VPAT (also asked for in Section 4) or any accessibility policies provided by the vendor.