****

**Third-Party Instructional Tool
Information Assurance Guidance**

**Background**

Instructors are increasingly able to incorporate new technologies and software into their classes as low or no-cost options proliferate. The innovative integration of emerging technologies, including some that may be commercial offerings, into classes across all disciplines is what U-M students expect from world-class faculty. However, when these tools are hosted or developed by a non-U-M third-party vendor, instructors should not assume that they have been institutionally scrutinized for compliance with relevant policy, privacy, security, and legal requirements. Consequently, it is important that instructors conduct a good faith effort to ensure that the most critical compliance risks are reasonably accounted for *before* making a third-party tool a required component of a class.

This document identifies common issues and risks when using such third-party tools in instruction, and provides recommendations to reduce the risks associated with them. Instructors should weigh the needs of the course activity against risks related to *privacy, security, record availability and backup, IT systems support*, *intellectual property,* and *accessibility*. Non-U-M providers of third-party tools and services may have policies and practices that do not meet U-M, state, federal, and other specific data protection regulatory requirements.

**Instructions:**

1. Instructors should communicate to students in the syllabus and at the start of a class whether use of non-U-M tools will be part of the standard class requirements or optional. This should include an explanation about what kind of data, if any, will be collected, for what purpose, and whether students can opt out of use of the tool. Other core instructor expectations are listed in the main body of the document.
2. The core expectations to be accommodated by a prospective software vendor are outlined in Appendix 2. The vendor should comply with these provisions before implementing its tool on a CTools site.
3. Web sites that provide additional information on the policies, standards, and regulations that support the guidance below are provided in the **Additional Resources** chart (Appendix 1). In addition, contact information for relevant **University Offices** is also listed in Appendix 3.

**General Use**

*Mandatory v. Optional Participation*

* Use of non-U-M tools should not create an unnecessary burden for students who do not agree with the third-party's policies and practices (also see the Privacy section below).

*Notice and Communication*

* Provide sufficient advance notice to students (e.g., in a course syllabus or via a click-through window) when their data will be collected, processed, or stored by any technology tool not fully under U-M’s control. This allows a student to decide whether to withdraw from the course, or request alternate solutions when withdrawal from the course may not be possible.

**Privacy and Use of Data**

## General

* Restrict the third-party site only to members of the class.
* If there are important pedagogical reasons for the site to be open the public at large (e.g., an online art gallery where public critique is important), it is recommended that instructors:
	+ Not require students to post personally identifiable information on the publicly accessible site.
	+ Suggest that students use aliases when creating accounts for non-U-M tools if access to student work will be public.

## Data Classification

* Many personally identifiable information elements are protected by laws, regulations, and U-M policies. U-M’s data classification standard identifies these elements and classifies them as "sensitive." Some of these elements include:

|  |  |
| --- | --- |
| * Social Security numbers
* Credit card numbers
* Debit card numbers
* Bank account/financial account numbers
* Driver's license numbers
 | * State ID card numbers
* Student loan information
* Health and medical information
* Passphrases/passwords, PINs, and security/access codes
 |

* Avoid collecting, processing or disclosing sensitive data via non-U-M tools.
* Personal health information (PHI) should not be collected, processed, disclosed or stored using the third party tool.

*FERPA*

* The Family Educational Rights and Privacy Act (FERPA) does not prohibit instructors from having students use third-party tools as part of their course activities.
* If it is necessary for the instructor to disclose FERPA-protected student education records to the non-U-M tool to meet pedagogical objectives, U-M must contractually require the service provider to comply with FERPA as a “school official.” Contact the General Counsel's Office first for assistance in this process.

**Information Security**

*Access and account restrictions*

* Remind students not to use their SSNs or U-M usernames and passphrases when creating accounts.
* If consistent with pedagogical objectives, instructors should, whenever possible, restrict access to student content on non-U-M tools to those enrolled or involved with the course. The tool should allow this capability.
* Advise students to limit their postings to course-related content, and that any use of the tool for non-course-related purposes should be considered outside the scope of the course.
* Delete student content from third-party tools when no longer needed (but be aware, and make students aware, that doing so may not remove such content from the third-party's archives caches or search engine results).

**Payment Card Data Processing**

The payment card industry (PCI) has a defined set of data security standards (PCI-DSS) that govern how payment cards must be processed.

* If U-M systems will be used to process or store payment card information then the instructor must contact the University Treasurer’s Office. The University Treasurer’s Office/Card Services is responsible for the coordination of any e-commerce projects with the various internal departments and the University’s Merchant Acquirer Processor.
IF NOT
* If instructors wish to process payment card industry data via a third party, then they should take the following steps:
	+ Take steps to ensure that the vendor is PCI compliant by requiring proof of vendor certification and incorporate that certification into a contract before any allowing for the vendor to process payment card data.
	+ Make it clear to the end-user that payment card transactions are NOT being processed by U-M.
	+ Ensure that U-M systems are not involved in the storage, processing or transmittal of payment card data.

**Data Back-up and Recovery**

* Some U-M data is typically subject to Freedom of Information Act requests and other public records law, regardless of where they are stored. Instructors should ensure that data, if necessary, may be retrieved from the non-U-M service provider.
* Many providers assume no responsibility for backing-up content; instructors should ensure that data backup is built into the vendor agreement or ensure that data residing on non-U-M tools and services is regularly backed up.

**IT System Support**

* Because of unfamiliarity with the tool, or lack of access to the underlying technical configuration, U-M help desks will not be able to help instructors or students troubleshoot and resolve issues. Instructors and students will need to rely on the third-party directly, or on other outside support, for assistance.
* Instructors should be aware of the third-party support options available, such as help desk phone, e-mail support, or user forums. It is desirable to experiment with using these options prior to committing to use the non-U-M tool to help determine whether they will meet class participant needs.

**Terms of Service**

* Providers of non-U-M tools may require users to "click through" an agreement that enumerates specific “Terms of Service” or “Terms of Use.” These terms are generally considered legally binding on the users; therefore, it is important that users (including instructors assigning students to use a third-party tool as part of a class) read these terms carefully. Instructors should consult with the General Counsel's Office if they do not understand any of those terms or their potential impact on students and their activities.
* Class participants should be informed in a straightforward, transparent manner when they are leaving the CTools site to be taken to a third-party site that will require them to submit personal information or fill out any kind of form or registration.
* “Click through” agreements should NOT be used for services that process, transmit, or store data classified as sensitive under the U-M data classification standard.
* Providers of non-U-M tools may reserve the right to change their Terms of Service at will and without notice to users. Instructors should be aware of how changes are communicated, and monitor for changes, to ensure that the Terms of Service continue to be acceptable. Also, they should continue to explore alternative tools, in case the chosen tool chosen terminates or changes unacceptably prior to completion of the course.

**Contracts**

* Instructors are not authorized to enter into legal contracts on behalf of U-M. If a tool's Terms of Service or other agreement for accessing the tool requires an institutional signature, instructors should contact their unit’s key administrator.
* Be aware that even after a legal contract is signed, instructors and students may still be required to "click through" an End User License Agreement that obligates them to comply with particular rules or standards in their individual use of the tool.
* If the third party is processing/storing/transmitting data classified as sensitive under the U-M data classification standards, then a data protection agreement must be added to the contract or otherwise executed as an amendment to an existing contract or agreement.

**Intellectual Property**

* The University's technology transfer policy (formerly intellectual property policy) defines who owns the rights to content that is created or uploaded to the tool.
* Instructors should review the contract or Terms of Service agreement and ask the following questions:
	+ Who owns the intellectual property rights when content is created or uploaded to the application or service?
	+ Does the service provider claim any rights to use the content created or uploaded to the application or service?
	+ If there is a right of use claim, when and how are these rights terminated?
* Instructors should ensure that use of other copyrighted materials incorporated into content that they upload complies with copyright law, and instruct students to do the same.
* Instructors should recognize that placing content on a non-U-M tool might constitute "publication" in a manner that may inhibit publication of the work through other means (as may putting the content on a publicly available U-M website).

**For Additional Support and Consultation**

See Appendix 3 for a list of U-M offices that are available for additional support and consultation regarding different aspects of establishment an agreement with a third-party vendor. In general, instructors can start with the Information and Infrastructure Assurance Office for clarification of this guidance or response to specific questions or concerns.

Information and Infrastructure Assurance

Information and Technology Services

Last Revised: June 2011

**Appendix 1: Additional Resources**

|  |  |
| --- | --- |
| *U-M General Policies & Compliance** U-M Compliance Resource Center<http://compliance.umich.edu/>
* U-M IT Policies<http://cio.umich.edu/policy/>
 | *Learning and Teaching Resources for Faculty** Faculty Exploratory

<http://www.lib.umich.edu/faculty-exploratory>* U-M Teaching and Technology Collaborative<http://www.umich.edu/~teachtec>
 |
| *Data Classification** U-M Data Classification Overview (authorization required) (we should pursue removing the authorization required before issuing these guidelines)<https://www.safecomputing.umich.edu/umonly/dataClass.php>
* U-M Data Classifications Document (authorization required)<https://www.safecomputing.umich.edu/umonly/documents/Data%20Classifications.pdf>
* U-M Sensitive Data Examples<http://safecomputing.umich.edu/main/sensitiveData.html>
* U-M Information Asset Classification Guidelines (draft)<https://www.safecomputing.umich.edu/umonly/documents/Information%20Asset%20Classification%20Guidelines.pdf>
 | *Higher Education: 3rd Party Vendor Guidance** U-M Cloud Computing Guidelines<https://www.safecomputing.umich.edu/umonly/cloud_computing.html>
* Indiana University: Use of Social Networks, Blogs, Wikis, and Other Third-Party Hosted Tools in Instruction[http://www.teaching.U-Mb.edu/finder/wrapper.php?inc\_id=s2\_6\_tech\_04\_cloud.shtml](http://www.teaching.iub.edu/finder/wrapper.php?inc_id=s2_6_tech_04_cloud.shtml)
* U-W Madison: Guidelines for Use of Applications and Service for Instruction<http://www.cio.wisc.edu/policies/Non-UWAppsServicesInstruction.doc>
* Cal-Berkeley IT Service Provider Privacy and Confidentiality Responsibilities<https://technology.berkeley.edu/privacy/#it_service_provider>
* Stanford Application Service Provider (ASP) Information Security Questionnaire<http://www.stanford.edu/dept/Internal-Audit/infosec/Stanford_ASP_Stds.html>
* Stanford Standard Application Service Provider (ASP) Security Clause<http://www.stanford.edu/group/security/securecomputing/ASP_security.html>
 |
| *Family Educational Rights and Privacy Act (FERPA)** Dept. of Education FERPA Homepage<http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
* U-M Student Rights and Student Records Policy<http://ro.umich.edu/ferpa/>
* Office of General Counsel Guidelines

 <http://www.ogc.umich.edu/faq_student.html> | *Payment Card Industry Standards** PCI Security Standards Council<https://www.pcisecuritystandards.org/index.php>
* PCI Standards<https://www.pcisecuritystandards.org/security_standards/documents.php>
* Acceptance of Credit Card Payments (U-M Standard Practice Guide)

 <http://spg.umich.edu/pdf/501.06.pdf> |
| *Intellectual Property & Copyright Guidance** U-M Technology Transfer Policy (Intellectual Property)<http://www.techtransfer.umich.edu/resources/policies.php>
* U-M Copyright <http://www.lib.umich.edu/copyright>
* U-M Copyright Policy (SPG 301.3-2)<http://spg.umich.edu/pdf/601.03-2.pdf>
* Creative Commons

<http://creativecommons.org> | *Americans with Disabilities Act (ADA)** U-M Campus Disability Resource Directory<http://www.umich.edu/Disability/>
* Office of Services for Students with Disabilities

<http://ssd.umich.edu>* Adaptive Technology Computing

<http://www.igtcs.umich.edu/atcs> * Web Accessibility

<http://www.umich.edu/webaccess> |

**Appendix 2: Guidance for Service Providers**

**Background**

University of Michigan service providers should abide by the core privacy and security expectations enumerated below when collecting, processing, sharing, storing, and disposing of U-M provided data.

**Protection of University Data**

Vendors must comply with all applicable federal, state and local law and regulations pertaining to the use, disclosure, storage, handling, and transmission of University data; vendors should maintain an information security program that meets or exceeds industry standards and best practices.

**Privacy and Use of Data**

Vendors are proscribed from use of University data for any purpose, including sales solicitation or other marketing not expressly agreed to in advance by the University. Permissible use of data—with advance permission of the University—may include surveying class participants for purposes of evaluating a web-based tool or other content that was part of a CTools course site.

**Payment Card Data Processing**

If a vendor will process credit card payments, the vendor must be PCI compliant and provide evidence of their PCI certification.

**Data Back-up and Recovery**

Vendors must ensure that data residing on non-U-M tools and services are regularly backed up as part of their ongoing backup and recovery processes. The vendor should describe/document their data backup practices and how data can be accessed and recovered.

**Terms of Service**

End-users should be informed in a straightforward, transparent manner when they are leaving the U-M CTools site and taken to a third-party site that will require them to submit personal information or fill out any kind of form or registration. Sample language that can be used when students are expected to “click through” to a third-party web site: “By continuing past this page to the [fill in the vendor site name], you are leaving the University of Michigan IT environment.”

**Accessibility and the Americans with Disabilities Act**

Third-party tools or content required for a course should meet or exceed current web content accessibility guidelines unless the instructor is providing a reasonable accommodation.

**Indemnification**

Vendor indemnifies, and holds harmless the University from any breach arising from this agreement or any negligent acts or omissions of the vendor.

**Security Incident Notification**

Vendor is required to notify the University of any unauthorized use or disclosure, or reasonable belief of disclosure, of any University data. Notification is to take place within 24 hours after knowledge of the suspected breach.

**Appendix 3: University Offices**

**Freedom of Information Office**

<http://www.vpcomm.umich.edu/foia.html>

patsell@umich.edu

734-763-5082

**General Counsel**

<http://www.ogc.umich.edu>

ovpgc@umich.edu

734-764-0304

**Information and Infrastructure Assurance**

<http://safecomputing.umich.edu>

Sol Berman, Manager, IT Policy, Privacy, Enterprise Continuity, and User Advocate, solb@umich.edu, 734-647-9661

Alan Levy, IT Policy and Compliance Lead, ajlevy@umich.edu, 734-647-5357

Kirk Soluk, Manager, IT Security Services, kmsoluk@umich.edu, 734-615-0301

**Technology Management Office**

<http://www.techtransfer.umich.edu/resources/policies_overview.php>

techtransfer@umich.edu

734-763-0614

**Treasurer’s Office**

<http://www.finance.umich.edu/treasury>

treasury@umich.edu

734-763-2201