



# Third-Party Educational Technology Guidelines

## University of Missouri-Columbia

These guidelines help ensure that educational applications hosted off-campus comply with guidelines and policies of the University of Missouri – Columbia.

### General

- 1) Non-MU parties wishing to provide externally hosted educational applications for MU faculty and students should contact Educational Technologies at Missouri (ET@MO): [etatmo@missouri.edu](mailto:etatmo@missouri.edu)
- 2) To ensure that the University has at least the minimum amount of information needed to evaluate whether the application meets the University's policies and needs, vendors will be asked to provide basic information addressing specific areas of concern outlined in "ET Vendor Questionnaire" and "ASP Standards" files.
- 3) Vendors should provide a copy of their privacy policy and user agreements that apply to the technologies and services involved.
- 4) The principal points that the University will consider concern overlap with existing campus systems, privacy, security, data retention, compatibility, and support.
- 5) Students and faculty should be provided with free and convenient support.
- 6) Any direct costs to students, faculty, or the University must be specified.

### Privacy and the Family Educational Rights and Privacy Act (FERPA)

- 1) Vendors should be sensitive to, and must adhere to, FERPA.
- 2) Unless students need to pay for portions of the application by credit/debit card, they should only be required to provide name and an email address when registering for or using the application. They should never be required to provide their student number or SSN.
- 3) Students and faculty in one course must not be able to see identifiable information (including names) of students in another course.
- 4) Tools and content areas should be able to be turned off or restricted by the instructor, both to allow shutting off areas that may violate MU's policies with regard to FERPA and to prevent confusion with tools that duplicate functionality already provided by the University.
- 5) When registering or logging in for the first time, students should be notified that they are on a non-university site.

### Security

- 1) Due to security and privacy concerns, MU prefers to host applications on campus when feasible. The availability to host locally may affect decisions about the use of an application.
- 2) MU should be informed when a vendor uses a third party to host or develop applications. Third-party hosting may be a factor in decisions about using an application.
- 3) All data transmissions containing FERPA protected data or other sensitive data shall be encrypted. All transmission protocols used between systems shall be explicitly indicated.
- 4) One-way, pass-through authentication from Blackboard, WebCT CE, or Sakai is preferred. If it is not available, a supported campus authentication service (Active Directory, LDAP, or Shibboleth) is preferred to vendor only authentication solutions. In the case of a vendor provided authentication scheme vendors shall provide information on the requirements and management practices associated with usernames and passwords.
- 5) For off-campus hosted solutions the vendor shall provide information related to vulnerability management of their networks, systems and applications as well as appropriate documentation to support the vendor's use of defense in depth strategies related to information security for their product.

### Data Retention

- 1) MU normally retains all student and faculty data in educational applications at the end of each semester for at least five years. If a vendor maintains it for less than five years (on or offline), then MU will need to know how long the data is maintained by the company and will need a means of obtaining that data for retention.
- 2) Vendors should provide information on their backup and restoration policies and procedures. Please be specific regarding what data is retained, who has access to it, and what steps are taken to ensure FERPA compliance.

### Compatibility

- 1) Vendors will need to provide information about the compatibility of their applications with different operating systems. Minimum versions of operating systems, browsers, plug-ins, or other required software (or of hardware) must be provided.
- 2) The application must be ADA compliant.