# **Procedure 918: Procedure for Faculty Use of Third-Party Tools in Courses**

Category: Instruction

Covered Individuals: CEI Faculty

Approved: 9/3/2024

Formerly Approved: 7/29/2024

**918.1 Procedure**

The faculty at the College of Eastern Idaho may utilize third-party tools to enhance educational experiences. While these resources can be beneficial, they pose potential security risks, particularly those requiring personal data for account creation. This document provides a framework for faculty to responsibly incorporate such tools into their curriculum.

**Definition of Third-Party Tools:**

A third-party tool is any software, service, or website developed by an external company that is used to support the needs of the college. These tools are not created by the educational institution itself but can be integrated into the institution’s systems to enhance the educational experience. These tools typically need user data such as email addresses, names, or other personal information to create an account and provide access to its services. ​

1. **Risk Assessment**
	* **Legal, Regulatory, and Compliance Risks**: Usage of third-party services may impact legal standards and institutional agreements, including GDPR and FERPA.
	* **Cybersecurity Risks**: There is an inherent risk of cyber threats and data breaches associated with third-party tools.
2. **Faculty Responsibilities**
	* **Approval Requirement**: Faculty must obtain authorization via Third-Party Tool Request Form (located in the SoftDocs Central Forms) from IT, their Department Chair, and Dean before integrating a third-party tool into their course. Submission deadlines are:
		+ April 30th for the Fall Semester
		+ October 31st for the Spring Semester
	* **Vetting Process**: The CEI Cybersecurity team will evaluate the tool’s security, compliance, and accessibility pre-departmental approval. Upon completion of the vetting process, all involved parties will receive notification regarding the final approval status of the tool.
	* **Disclosure**: Faculty are required to:
		+ Inform students about any third-party tool usage and associated costs.
		+ Report security incidents related to third-party tools to the IT department.
3. **Best Practices**
	* **Regular Audits**: IT will conduct annual reviews of third-party tools to ensure ongoing compliance with CEI security standards. Non-compliant tools may be removed from the approved list.
4. **Process and Procedure Changes:** During updates to processes and procedures Deans, in collaboration with IT, may issue new instructions that must be followed. These instructions can be communicated verbally or electronically to the faculty. It is implicitly understood that maintaining the security of the college’s data is the highest priority during these transitions.
5. **Noncompliance**
	* **Immediate Written Warning** Because the vulnerability of the college infrastructure may become compromised, faculty members who disregard these procedures will receive a written warning, skipping the verbal warning phase, due to the nature of the violation of this procedure.
	* **Dismissal**: Persistent noncompliance or a single incident leading to a security breach may result in dismissal. Dismissal decisions will adhere to the college’s disciplinary protocols, potentially involving evaluations by the Department Chair, Dean, and HR Department.
	* Dean’s Responsibilities: The Dean to whom the faculty member reports is responsible for initiating disciplinary actions. Depending on the severity of the offense, the Dean may seek guidance from the IT department to assess the impact and determine appropriate measures.