CTL Educational Technology Systems Integration Policy

Scope

This policy applies to all faculty, staff, students, and affiliates who request an integration with the Center for Teaching and Learning (CTL) managed educational technologies with other platforms.

Policy Statement

CTL will review and implement educational technology integrations based on RIT policies, standards, and practices. System level integrations will require full reviews of the requested systems including contractual agreements and signatures. RIT instructors are responsible for conducting reviews of course-level integrations.

Rationale

CTL provides RIT instructors access to the technology and data required to support teaching at the highest standards. The goal is to provide access to CTL-managed systems where appropriate in alignment with RIT Procurement, Data, and Security standards. Instructors may request integrations of third-party services with CTL-managed systems to support their teaching if requests meet CTL's requirements:

1. Business needs and third-party agreements have been approved by the appropriate offices and business owners.
2. A security review of the integration is completed with the RIT Information Security Office.
3. Integrations must not require a privileged service account.
4. Integrations must adhere to standards that are actively maintained for security.
5. There is an understanding that CTL will continually audit and review integrations and CTL reserves the right to disable any integration based on third-party compliance or security concerns.

Procedures

LTI (Learning Tools Interoperability) Integration Requests

Completing the integration request will take approximately a full semester and is dependent on the volume of current requests and workload across offices at RIT as well as vendor responsiveness and completeness of their provided documentation and agreements (HECVAT, SOC2, NDA, DPA).

Integration requests must be submitted via CTL and must include the following:

- Requester will provide approvals on master agreement and/or terms of service and a completed RIT Data Sharing Agreement.
- The requester will be responsible for gathering any documentation needed by the ISO to conduct the review including the vendor HECVAT and SOC2.
- The requester must complete an ITS Information and Access and Protection Questionnaire (IAPQ) to initiate an ISO review. This document will need to be signed by the Dean or AVP as the Primary Business Process Owner. Other supporting documentation may be required to complete the review.
- If the ISO identifies required security controls, CTL will not release the integration until the requester has implemented and verified those controls.
- If it is determined that a Data Processing Addendum (DPA) will be necessary, the requester must complete the form and secure the required signatures.

Once all the above steps are completed and approved, CTL will proceed with the technical integration. (NOTE: CTL does not provide support for any third party integrations that are not designated as a CTL-supported technology.)

API (Application Programming Interface) Access

API requests will follow the same steps and procedures as LTI requests, however, these requests require some additional review including:

- Account level access review: API access will be restricted to current level of access defined by current user privileges.
    - The requester will also provide a list of required functions needed for the application. These will be used to further limit the scope of access for the API configuration.
- Privileged API access will require additional ISO reviews and Academics Domain Steward approval.
- CTL supports the provisioning of API access but does support the requester's application.
- Student projects requesting API access will require a faculty sponsor with appropriate signatures for data stewards defined in RIT's data governance standards.
- API requests may require additional reviews and may be limited in scope and duration of activity.

Existing Integrations and APIs

On a 12-month recurring basis, CTL will review to determine if existing integrations and API access provision are still valid based on:

- Confirmation from the Primary Business Process Owner that access is still being utilized
- Verify that all ISO-recommended controls are still in place
- Validation that the existing implementation still meets current standards

This process will enable CTL to update records for when the Primary Business Process Owner changes. Based on review, CTL may revoke access or disable the integration.

Responsible: Office of the Provost

Effective Date: July 1, 2026

Policy History
Approved - April 1, 2026