

CTL Educational Technology Systems Access Management Policy

Scope

This policy applies to all faculty, staff, students, and affiliates who access educational technology systems managed by the Center for Teaching and Learning (CTL).

Policy Statement

All systems managed by CTL require an RIT Account for access via enterprise identity and access management services. Local accounts will only be provided for internal CTL administrative business needs. Access privileges and roles will be assigned based on the users' responsibilities and in accordance with [RIT's Account Management Standard](#).

Rationale

CTL has adopted this policy to adhere to principles outlined in [RIT's Account Management Standard](#).

Procedures

Academic Technology Systems Roles

SIS-listed course roles within CTL's managed systems are assigned based on role definitions provided in RIT's Student Information System (SIS). RIT instructors are permitted to add existing RIT users to courses they manage and assign appropriate roles within their course. A full description of roles can be found in: [What access is granted to each Role in a myCourses course?](#)

Requestors of non-SIS listed course shells are assigned a Course Administrator role to ensure appropriate access to RIT Private and Confidential data.

Academic Technology Systems Service Accounts

Accounts that need privileged access to CTL-managed systems may be requested. These requests will be evaluated by CTL and ITS/ISO as needed to ensure appropriate access to RIT Private and Confidential data.

Course Access Requests

Instructors are responsible for granting course access in systems where they are able to manage enrollments. Users with the *Hidden Instructor* role can also grant course access when appropriate. In all other circumstances, CTL can provide access upon receiving written approval from the appropriate department head.

Access for Users Without Existing RIT Accounts

Users needing access to RIT's educational technologies who do not hold an active Faculty, Staff, Student, or Retiree account must request the linking of an external ID with RIT or have a RIT Account of Affiliate type created and imported. External ID and Affiliate type accounts are classified as either External Learner or Approved Guest and provided permission based on their associated group as follows:

All account provisions not covered by these standard procedures require review and approval by the Executive Director of CTL.

External Learner

This role is for non-RIT users participating in non-credit, RIT-sponsored courses, certificate offerings, or outreach programs.

- Enrollment into courses must be requested by an Associate Dean and approved by the Executive Director of CTL.
- CTL staff will manually enroll these users
- Instructors cannot enroll External Learners to courses.
- External Learners possess standard student-level access within their enrolled courses.

Approved Guest

Approved Guest accounts are intended to provide access for visiting instructors, external course support staff, and visiting scholars. Prior to external accounts being provided the Approved Guest role, the account requester will need to have the appropriate approvals in place:

- Requests for Approved Guest access must come from the department head or director.
- Dean or Vice President signed Non-Disclosure Agreements (NDA) are mandatory for all users being provided an Approved Guest account. NDAs are required due to the ability for instructors to enroll Approved Guests into RIT Courses that contain private and confidential data.
- Users entering credit-bearing courses or courses with active RIT students are subject to additional reviews to ensure compliance and appropriate access levels.
- CTL will not grant access until NDA completion is confirmed.

Academic Technology Support Staff Privileged Accounts

While Brightspace (RIT's LMS known as myCourses) does leverage role-based access at the system and course levels, CTL will create local administrative accounts for internal staff and student employees in support roles. These accounts are required to use multi-factor authentication and are disabled when the user's employment with CTL ends.

For privileged CTL support student employee accounts in myCourses, CTL will conduct an audit twice a semester to ensure there are no inappropriate uses of the privileges. CTL will check to

ensure that no grades have been modified, that there has been no privileged access to any courses the student employees take or have taken, and that all access is during expected work hours.

Account Deletion

CTL does not actively delete accounts from any of the supported systems unless account removal is required to meet data retention schedules. CTL will follow the guidelines provided by General Data Protection Regulation (GDPR) for requests coming from residents of the European Union.

By leveraging enterprise authentication services, access to systems by users that are no longer members of the RIT Community will be automatically revoked.

Definitions

Standard User-Level myCourses Roles (Instructor, Student, Teaching Assistant) are documented in: [What access is granted to each Role in a myCourses course?](#)

Related Policies and Standards

[RIT's Account Management Standard.](#)

Responsible: Office of the Provost

Effective Date: July 1, 2026

Policy History

Approved - April 1, 2026