Third-Party OAuth Application Policy

Policy number: 800-IT-8
Policy owner: Information Technology Services

Date of initial publication: August 20, 2026
Date of latest revision: N/A

SECTION I. PURPOSE

This policy establishes the criteria the university uses to allow, review, deny, and periodically reevaluate third-party OAuth applications that request permission to access university accounts or data.

This policy is intended to control which third-party OAuth applications may integrate with the university's identity system and to protect university accounts and data.

SECTION II. SCOPE AND APPLICABILITY

This policy governs third-party OAuth applications that use the Open Authorization framework to request permission to access a user's university account or data.

The requirements in this policy apply to applications that request authentication-only access or access to email, contacts, calendars, files, storage, or other university data.

SECTION III. DEFINITIONS

When used in this policy, the following term has the following meaning:

> ***OAuth application*** means a third-party service or software that uses the Open Authorization framework to request permission to access a user's university account or data. Depending on the scopes requested, an OAuth application may gain access to email, contacts, calendars, files, or other university data. Even "sign-in only" permissions use the same framework, which requires the university to control which applications may integrate with its identity system.

SECTION IV. APPLICATION APPROVAL AND REVIEW

A. Authentication-Only, Microsoft-Verified Applications

Applications that request authentication only and are published by a Microsoft-verified publisher are allowed. These applications do not require additional review because they do not access university data and their publisher identity has been validated by Microsoft.

B. Applications Requiring Review

Any application that does not meet the criteria in Section IV.A will undergo review. This includes:

a. Applications requesting access to email, files, contacts, calendars, storage, or any other user or university data.

b. Applications requesting persistent or elevated permissions.

c. Applications whose publisher is not verified by Microsoft.

d. Applications from vendors with whom the university has no existing contract or data protection agreement.

C. Limited Set of Widely Trusted Applications

A small number of widely used and industry-standard applications, such as the native iPhone Mail and Android Mail clients, are allowed due to their established security posture, broad necessity, and long-standing trust record.

D. Default Denial for All Other Applications

If an application falls outside the permitted categories and does not pass review, it will be denied by default. Exceptions may require documented business justification, a formal risk assessment, and confirmation that contractual protections exist. Requests for exceptions can be submitted to the ITS Tech Desk and will be reviewed by the CISO or their delegate.

SECTION V. PERIODIC REVIEW

Approved applications are subject to ongoing evaluation. Changes in publisher verification status, ownership, data practices, or requested permission scopes may result in access being revoked.