UNIVERSITY OF CENTRAL FLORIDA

University Standards

Subject:	Enterprise Application Standard for Third Party Application Integrations with Office 365
Standards Number:	503
Effective Date:	2/20/2026
Revised Date:	2/20/2026
Responsible Authority:	Holly Drake, Chief Information Security Officer
Pages:	4

ACCOUNTABILITY:

Any UCF faculty, staff, or student seeking to provide a third-party application access to their UCF Office365 email or information by using their UCF account to sign in.

APPLICABILITY:

This standard applies to any user-initiated request for a third-party application seeking permissions to integrate with the user's Office365 email and/or data. There are two categories of third-party applications. The first category of third-party applications is considered "verified applications" because they are Microsoft trusted and only request pre-approved permissions. The second category includes non-verified third-party applications or applications that request a permission level higher than the pre-approved base level permissions. Sometimes users call these features add-ins or add-ons.

STANDARDS STATEMENT:

UCF constituents that use Office365 have a desire to use applications that request permission to access an account's resources and data (e.g., email, calendar, and OneDrive data) via an integration that uses a Microsoft Graph Connection. UCF recognizes that allowing certain applications to synchronize data can enhance the experience for individuals. However, these applications should adhere to the security and data governance requirements set in our policies and standards.

STANDARDS:

UCF allows user consent for applications from verified publishers, for selected permissions when requested via the Microsoft Enterprise Application Admin Consent workflow. Pre-approved applications are processed automatically and instantly. To be considered "pre-approved", the application must meet the following requirements.

1. The application must be a Microsoft Verified Publisher.

2. The application must request pre-approved permissions that do not provide access to email, calendar, or OneDrive content. Pre-approved permissions are listed here:

Interface	Permissions	Description
Microsoft Graph	**Email**	Allows the app to read your users' primary email address.
Microsoft Graph	**Offline Access**	Allows the app to see and update the data you gave it access to, even when users are not currently using the app. This does not give the app any additional permissions.
Microsoft Graph	**Open Id (Sign in)**	Allows users to sign in to the app with their work or school accounts and allows the app to see basic user profile information.
Microsoft Graph	**User Read**	Allows users to sign-in to the application, and allows the application to read the profile of signed-in users. It also allows the application to read basic company information of signed-in users.
Microsoft Graph	**Profile**	Allows the app to see your users' basic profile (e.g., name, picture, user name, email address).

Some third-party applications may ask for elevated permissions or are not developed by Microsoft Verified Publishers.
Third-party applications that do not meet the requirements above must be requested and are subject to review by a committee.

- The committee reviews the following information: purchase agreements, Vendor Risk Management (VRM) reviews, permissions being requested, justification, and any sanctioned technologies on lists provided from the Office of Foreign Assets Control (OFAC).
- Third-party applications that do not meet the pre-approved requirements (permissions and verified publishers) and request access to use AI or data (e.g., read, write, send, receive, etc. to applications such as email, calendar, and OneDrive) should be submitted through the vendor risk management (VRM) process first.
    - Requests made via the built-in Microsoft Enterprise Application Admin Consent process will be placed on hold until the VRM process is completed.
    - For reference, the full list of Microsoft Graph API (Application Programing Interface) permissions can be found here: https://learn.microsoft.com/en-us/graph/permissions-reference

Please note that departments who purchase applications must contact the Information Security Office to follow the Vendor Risk Management process and integrate NID Single Sign-On (SSO).

More information about the Vendor Risk Management (VRM) process can be found at Vendor Risk Management - UCF Information Security. All submissions must include the Secure Handling of UCF Data Questionnaire and any additional documentation depending on the classification of the data being shared with the vendor.

User Provided Justification

For requests to be considered, an adequate justification aligned to the needs of the University must be included. This justification will assist the committee in determining the benefits to UCF while considering any access permissions which the application is requesting.

Review Outcomes

Based on an evaluation of the information available, third-party application access requests are resolved using one of the following options:

1. Approve: Approves the third-party application's access to the requested Office365 data at the requested permissions level for any user in the enterprise who chooses to sign in using their NID account.
2. Deny: Denies the application request for the user.
3. Block: Denies the application for every user in the enterprise.

NOTE: Applications that request additional permissions will initiate a new administrative consent workflow and review.

The system notifies the user of the decision along with any relevant comments, if applicable.

Approved applications may be subject to future reviews and approval may be revoked.

Documentation

The committee will maintain documentation of application reviews and outcomes.

DEFINITIONS:

Microsoft Enterprise Application Admin Consent. A process where a user requests permission for an application to access certain data or perform specific actions on behalf of all users in an organization. Administrators must consent applications that require permissions that regular users cannot grant themselves.

Microsoft Graph. An interface tool that, with appropriate permissions, allows access to different parts of Microsoft's services, like email, calendars, and files. Both Microsoft and non-Microsoft applications can use Microsoft Graph to interact with different applications and services allowing the sharing and integration of information.

Microsoft Graph Connection. A logical container for external data that an administrator can manage. This connection allows applications to bring in data from various external sources, such as on-premises content or external Software as a Service applications, into Microsoft Graph.

Microsoft Verified Publisher. is a status given to application developers who have verified their identity with Microsoft. This verification process aims to ensure that the organization behind the application is authentic and trustworthy which reduces the risk of using potentially harmful applications. When an application is labeled as having a blue verified badge, it means that the developer has gone through a series of checks and has been confirmed by Microsoft as a legitimate.

RELATED DOCUMENTS:

Manage consent to applications and evaluate consent requests - Microsoft Entra ID | Microsoft Learn

CONTACTS:

Information Security Office https://infosec.ucf.edu infosec@ucf.edu	Security Incident Response Team (SIRT) https://infosec.ucf.edu/incident-response/ sirt@ucf.edu
Identity Access Management (IAM) https://infosec.ucf.edu/iam iam@ucf.edu	UCF IT Support Center (407) 823-5117 https://ucf.service-now.com/ucfit itsupport@ucf.edu

Revision Date	Summary of Change

INITIATING OFFICE: Information Security Office

STANDARDS APPROVAL

(For use by the Information Security Office)

Standards Number: 503

Initiating Office: Information Security Office

Chief Information Security Officer: Holly Drake

Signature: Holly Drake Digitally signed by Holly Drake Date: 2026.02.20 12:01:27 -05'00' Date: 2/20/26