Information Security Standard

Delegation of Microsoft 365 Permissions to Third Party Applications

I. Standard Statement

This standard operates under University Policy 117 Information Security Policy, ISO 27002 Controls 8.12 Data leakage prevention, and ISO 27002 Controls 8.3 Information Access Restriction. This standard defines and establishes the governance for application consent workflows and management of applications as it relates to those applications that that are attempting to access a protected resource such as reading the contents of a user's mailbox or having full access to a user's contact list.

II. Scope of this Standard

This standard applies to all users of Western Carolina University technology resources.

III. Definitions

A Malicious Application is an application that attempts to trick users into granting them access to your organization's data.

Banned Applications are applications that have been previously installed but have been deemed as malicious and therefore permissions have been disabled and future access revoked.

Consent is a process where users can grant permission for an application to access a protected resource.

A *Verified Publisher* means that the organization that publishes the app has been verified as authentic by Microsoft.

The *Admin Consent Team* shall consist of representatives from Operational Security, Vendor Management, Chief Technologist, EndPoint Management and the Cloud Applications teams

IV. Delegation of Permissions to Applications Standard

In order to protect from allowing unintentional access to protected resources by malicious applications the Division of Information Technology will apply a security feature to only allow users to consent to applications that Microsoft determines are low risk, from verified publishers or approved WCU applications. Applications that meet this standard will be considered approved by definition and will be inventoried and monitored by our WCU managed cloud security platform.

When a user attempts to install an application that does not comply with the above they will have the option to "Request Approval". This approval request will be sent via email to members of the Admin Consent Team for review. If the team deems the application is not malicious then they will approve the application and the user will be notified via email that their request was approved.

A. Reviewer Activity

Reviewers must be diligent in their review of an application. Reviewer activities would be the following:

- Review what permissions are being requested by the application
- The more common and used an app is, either by your organization or online, the more likely it is to be safe.

- An app should require only permissions that are related to the app's purpose.
- Apps that require high privileges or admin consent are more likely to be risky.
- Investigate user consents to the app in the activity log.
- Investigate the app's name and publisher in different app stores. Focus on following apps, which might be suspicions:
    - Apps with a low number of downloads. ○ Apps with a low rating or score or bad comments.
    - Apps with a suspicious publisher or website.
    - Apps whose last update isn't recent. This might indicate an app that is no longer supported.
    - Apps that have irrelevant permissions. This might indicate that an app is risky.
- If the reviewer is unable to determine if an application is safe then the Admin Consent team shall review.

B. Existing Applications

Applications that have already been installed will be reviewed to confirm they meet the standard. If an existing application does not meet this standard that application will be marked as “banned” having all permissions disabled for the application. Users of the application will be notified of the action and can request a review by contacting the IT Help Desk at 828-227-7487.

V. Exceptions and Review

Exceptions to this standard must be reviewed and approved by the Office of the CIO and/or the Information Security Privacy Council (ISPC).

This standard will be reviewed periodically and updated as necessary.

VI. References

International Standards Organization (ISO/IEC 27002:2022, Clause 5 Organizational Controls)

University Policy 117 Information Security