Roger Williams University

IT Policy: Use and Approval of Third-Party Add-ins and Plug-ins

Purpose

This policy outlines the procedures and requirements for requesting, evaluating, approving, and managing third-party add-ins and plug-ins across RWU's IT systems, particularly within the Microsoft 365 (O365) environment. The goal is to ensure security, compliance, accessibility, vendor accountability, and alignment with business objectives.

Scope

This policy applies to all employees, contractors, and third parties using organization-managed IT systems, services, and devices. It governs third-party software add-ins and plug-ins for:

- Microsoft Office applications (Outlook/Exchange, Word, Excel, etc.)
- Microsoft Teams
- SharePoint
- Web browsers (e.g., Chrome, Edge, Firefox)
- Other business-critical platforms

This policy also applies to third-party vendors or partners providing software that integrates with RWU's core IT platforms.

Definitions

Add-In / Plug-In: A software extension that adds specific capabilities to larger software platforms.

Approved Add-In: Any add-in that has been evaluated and authorized by IT Security and IT Governance.

Vendor Risk Assessment: A formal process to evaluate the information security, privacy, and operational risk associated with third-party providers.

User: Any individual accessing the organization's systems and requesting the use of third-party extensions.

Policy Requirements

Approval Process

All third-party add-ins and plug-ins must be approved by the IT department prior to installation or use. The requestor must submit:

- Name of the add-in/plug-in
- Vendor information (including contact and support details)
- Business justification
- Data access requirements
- App permissions (i.e. Scope)

Evaluation Criteria

IT will evaluate each request based on:

- Security risks (data access, permissions, vulnerabilities)
- Compliance with regulatory requirements (e.g., GDPR, HIPAA, FERPA, internal policies)
- Licensing and costs
- Vendor reputation and support
- Vendor risk posture and history of breaches or incidents
- Performance and stability impacts
- Data residency and integration with existing systems
- Alignment with institutional data governance and third-party risk frameworks

Restrictions

Add-ins or plug-ins will not be approved if they:

- Access or transmit sensitive or classified data without encryption
- Require excessive permissions (e.g., full mailbox read/write access)
- Are from unverified vendors or lack sufficient documentation
- Are not maintained or updated by the vendor
- Lack formal data protection agreements, or monetarize RWU's private data
- Fail to comply with accessibility standards

Usage Guidelines

- Only use IT-approved and centrally deployed add-ins.
- Do not self-install unauthorized plug-ins, even from trusted marketplaces like Microsoft AppSource or Chrome Web Store.
- Periodic reviews will be conducted to ensure continued relevance and compliance.
- Users must report any data exposure, service malfunction, or unauthorized behavior immediately.
- Vendors may be subject to periodic security re-evaluation, including HECVAT assessments.

Review and Auditing

IT Security will maintain a registry of all approved add-ins and plug-ins. This registry will be reviewed quarterly to:

- Remove unused or unsupported plug-ins
- Reassess existing permissions
- Confirm alignment with evolving business and regulatory needs
- Evaluate vendor compliance and performance

Violations

Unauthorized use of third-party add-ins may result in:

- Removal of the extension
- Disciplinary action

- Loss of access to O365 or other systems
- Reporting to legal or compliance functions if violations involve sensitive data

Exceptions

Any exceptions to this policy must be approved in writing by the CIO or IT Governance Board. Exceptions may require:

- Formal risk acceptance statements
- Compensating controls
- Time-bound usage with defined review points