Requesting Google Addons or Microsoft Add-ins

Kyle Oliveira - 2026-01-28 - Comments (0) - Google Workspace

OIT recognizes that Google Add-ons and Microsoft Add-ins can significantly boost productivity. However, because these tools often require access to your data—and by extension, Brown's Cloud data—they can introduce vulnerabilities if not properly vetted.

To ensure our community remains protected, we evaluate these tools to understand their full scope of access and functionality.

Before You Request: Check Approved Tools

Before submitting a new request, we strongly encourage you to review the suite of tools already vetted and available for use. You may find an approved solution that already meets your needs without the wait:

- **Google Add-ons:** Check the "**Approved for you**" section within the Google Workspace Marketplace.

- **Microsoft Add-ins:** Browse the integrated apps already available within your Office 365 interface.

Understanding the Review Process

Users should be aware of the complexities involved in the security review process. A successful approval depends heavily on the developer's transparency and responsiveness.

What you should expect:

- **Extended Turnaround Times:** Security reviews are thorough. Because we require detailed technical information from the developer, the process can take a significant amount of time.

- **Developer Dependency:** We often find that developers (particularly of "free" tools) may not respond to our security inquiries or may provide vague answers.

- **Possibility of Non-Fulfillment:** If a developer fails to provide satisfactory information regarding how they handle Brown's data, we cannot move forward with the installation. In these cases, the request may go unfulfilled.

How to Submit a Request

If you have verified that no existing tool meets your needs and you wish to proceed, you may submit a request to help@brown.edu or submit a request via the user portal. Include

any relevant data, including a link to the addon and its proper name.

To improve your chances of success:

1. **Provide Direct Contact Info:** You must provide a direct contact at the vendor/developer who can answer technical security questions.

2. **Verify Existing Contracts:** If the tool is part of an existing security-approved contract with Brown, please note that in your request so we can expedite verification.

3. **Business Justification:** Requests tied to specific departmental business needs or direct vendor partnerships often have a higher success rate for information gathering.

Alternative Options

If a tool cannot be approved for use with your Brown account, you may consider these alternatives:

- **Personal Accounts:** Use a personal @gmail.com or personal Microsoft account to use the add-on for non-sensitive, personal tasks.

- **Managed Computers (Microsoft):** If you are a faculty or staff member on a Brown-managed computer, you may be able to use certain add-ins via a differently licensed version of Office, provided they do not require Office 365 cloud access. See our guide for more details.