Stanford | University IT
Information Security Office

Position Paper - Use of non-University supported add-in/plug-in/applet software

Position Title	
Position Audience	Stanford Faculty, Staff, and Students
Contact	Information Security Office (https://stanford.service-now.com/it_services?id=sc_cat_item&sys_id=f7ae081a13bce2008a9175c36144b0ad)
Position Release Date	6/13/2022
Last Update	6/13/2022

Problem Statement

The University has a Data Risk Assessment (DRA) process for evaluating enterprise-supported use of software that involves High Risk data per Stanford's Data Risk Classification. In general, software that does not involve High Risk data is not required to undergo a full DRA review, rather such use is expected to comply with Minimum Security Standards and Minimum Privacy Standards requirements.

Many commonly used add-in, plug-in, and applet software (e.g., Grammarly, Calendly, etc.) are not licensed or supported by University IT (UIT) or campus IT departments, but are rather licensed (sometimes without cost) to individuals under end-user license agreements (EULA). As such, there is typically no formal IT support group to take ownership for enterprise use of such EULA-based software, work with the software vendor to collect sufficient details about how the software interacts with data (especially those associated with cloud-based services), or work with the vendor and/or users to implement any applicable security recommendations that may result from a DRA review.

Additionally, UIT lacks the granular administrative control capability to enable the use of specific cloud based add-in/plug-in/applet software (such as those for Microsoft Office365 or Google applications) without allowing such software to access any data repository for which that individual's SUNet ID is authorized to access. Furthermore, many data repositories (including email and local hard drives) contain unstructured data or a mixture of Low, Moderate, and High Risk data.

ISO Position

Unless a particular add-in, plug-in, or applet has undergone DRA review to ensure that an enterprise agreement and appropriate security controls are in place to protect Stanford data, individually licensed EULA add-in, plug-in, and applet software should not be installed and/or used to process any data in a repository that may contain High Risk data. For unstructured data repositories such as email or local hard drives, it is the user's responsibility to ensure that the add-in, plug-in, or applet is configured and/or used in a manner that no High Risk data is accessed. When no formal Stanford IT support is available, the user should reach out to the software vendor to determine how this can be accomplished.

For cloud-based software applications where the ability to install an add-in, plug-in, or applet is restricted, the user should determine whether a local client version of the software can be used (such as Microsoft Office) where the installation of a client version of the add-in, plug-in, or applet would not require additional privileges. This may also help limit what data the client version of the software is able to access.

Additionally, individually licensed third-party software should not be used to process the following types of High Risk data without explicit approval:

- Payment card information - which would be contrary to Stanford PCI Compliance requirements.
- Personal Health Information (PHI) - which requires that a Business Associate Agreement (BAA) be in place with the third-party vendor.