Security Standard for Add-on Marketplaces (SSAM) [SEC=UNCLASSIFIED]

The aim of these security requirements is to set a consistent standard across the industry to increase the protection of client data as well as improving portability of third party applications between different vendors. For example: Xero Marketplace, Myob Add-ons, Intuit Apps and Reckon Marketplace.

Implementation considerations		
Consideration	**End state**	**Guidance/specification**
Timeline	Give clarity for when these requirements apply	These requirements apply from: ● 1 July 2020 for those connections in place as at 31 December 2019. ● 1 January 2020 for all other connections.
Responsibility	Clear understanding of which party needs to undertake a given action and when	**Third party app store developers:** ● with more than 1,000 connections to Australian small business customers of a DSP, or is ● connected to the practice client list of an Australian tax or BAS agent (practice connection) ● should provide a completed self-assessment on an annual basis to that DSP **The DSP should, as part of their annual certification with the ATO under the Operational Framework, provide:** ● a list of the applicable third party app store developers with more than 1000 small business connections or a connection to tax agent/practice client list (including individuals); ● the date the self-assessment has been completed; ● confirmation that the self-assessment has been approved by the DSP; and ● details of any outstanding matters
Non-compliance	Ensure an opportunity to remediate and clarity of required actions for non-compliance	**Where a third party app store developer does not adequately comply with these specifications:** ● the DSP will issue them written notice giving them 30 days to advise the treatment plan and up to a further 60 days to complete the required work.

Security Requirements		
Requirement	**End state**	**Guidance/specification**
Encryption key management	Ensure effective key management is implemented to protect client data.	Verify that your app meets these requirements for OAuth token management. ● OAuth tokens or customer-identifying information must not be exposed within your app or shared with other parties. ● Token management once a user completes the OAuth authorization workflow: o OAuth 1.0a ▪ Encrypt and store the consumer key, consumer secret, access token and access token secret in persistent memory. ▪ Encrypt the access token with a symmetric algorithm (3DES or AES). AES-128 or greater is preferred. ▪ Store your AES key in your app, in a separate configuration file. o OAuth 2.0 ▪ Encrypt and store the refresh token in persistent memory. ▪ Encrypt the refresh token with a symmetric algorithm (3DES or AES). AES-128 or greater is preferred. ▪ Store your AES key in your app, in a separate configuration file.
Encryption in transit	Ensure that sensitive client data in your app is protected during the transport process.	(MANDATORY) App server is configured using SSL to support only TLS version 1.1 or higher. (RECOMMENDED) TLS version 1.2 using AES 256 or higher with SHA-256. Web application endpoints that receive sensitive customer information and/or authentication tokens in URL parameters must not return HTML content via an HTTP Response Body. This is to prevent sensitive customer information from being accidentally leaked to 3rd parties in the subsequent HTTP Referrer request headers. Instead, the web application endpoints should implement a 302 Found redirect. This is particularly important when application end points are handling authentication tokens.
Authentication	Ensure that users who access to your app are authenticated.	Ensure that strong customer authentication is enabled (minimum two step authentication or single sign on).

Indirect access to data	Ensure that unauthorised third-parties are unable to access customer data.	Third party access to customer data must be clearly stated within applicable policies and/or terms and conditions, and have a justifiable business need. Note: ● Third party access may include access via an external API, or through data that is stored. ● Justifiable business need may include (but not limited to) the utilisation of third party services, which is functionally required. For example, the use of third party biometric services.
App server configuration	Ensure that your app server is secure.	Ensure your server's configuration follows industry accepted hardening practice for example: ● National Institute of Standards and Technology – Guide to General Server Security ● Relevant vendor recommendations
Vulnerability management	Ensure that your app is secure against the common vulnerabilities.	Follow an industry accepted standard for secure code development such as OWASP Top 10 to protect against vulnerabilities such as: ● Cross Site Request Forgery ● Cross Site Scripting (including reflected and stored cross site scripting) ● SQL Injection ● XML Injection ● Authentication, Sessions Management and Functional level access control (if any) ● Forwards or Redirects in use have been validated ● All app session cookies have the following attributes set: Secure and HTTPOnly
Encryption at rest	Ensure that sensitive client data in your app is protected while at rest.	Encryption at rest using NIST Cryptographic Mechanisms is mandatory for data repositories that hold or manage sensitive commercial or personal information. Examples may include; full-disk, container, application or database level encryption techniques. We define sensitive commercial or personal information as information which if disclosed could cause harm to the individual or organisation. Examples include:

		• Personal - date of birth, tax file number, address, income, biometric, credit history etc. • Commercial - financial, transactions, accounts, trade secrets etc.
Audit logging	Ensure appropriate audit logging functionality is implemented and maintained.	Audit logging should include both application level (access logs) and event based actions. You should consider your environment and what logging should be implemented and ensure that the logging records include the following where applicable: • Date and time of the event • Relevant user or process • Event description • Success or failure of the event • Event source e.g. application name • ICT equipment location and identification Audit logs must be retained for as long as appropriate to enable future investigation. In most cases logs should be kept for a minimum of one year. Logs must be immutable and secure.
Data hosting	Ensure client data is not hosted in high risk areas.	Consideration needs to be given to country, legal, contractual, access, sovereignty and counter-party risks.
Security monitoring practices and breach reporting	Ensure you have security monitoring practices in place to detect and manage threats.	You need to be able to demonstrate that you scan your environment for threats and that you take appropriate action where you detect anomalies. Monitoring can be at the: network / infrastructure, application or transaction (data) layer. Where anomalies are detected you must report these to the DSP, providing enough information to enable further monitoring and/or preventative action.

Approval date: Wednesday 14 August 2019