Beautiful business

SAMPLE

Xero API Consumer Annual Security Assessment

Confidential(p)

Beautiful business

Xero API Consumer Annual Security Assessment Sample Document

What is the Xero API Consumer Annual Security Assessment?

The Xero API Consumer Annual Security Assessment must be passed in order to gain access to the Xero Practice Manager API. The assessment is 21 questions long, and must be passed yearly to maintain your access. You may be required to implement changes if you don't meet the needed criteria, such as MFA on all user accounts, coding and hardening practices, and storing tokens securely. Please see our post on raising our platform's global security standards, and see our security standard for API consumers, for more details.

How do I get to the Xero API Consumer Annual Security Assessment?

Complete and submit the Xero Practice Manager API Access Form. The security assessment will be sent to you by a member of our team after submitting this form.

Xero API Consumer Annual Security Assessment Sample

Section 1 API Consumer Information

1.1 Who do you work for?

Please use the full registered company name. This can generally be found on your website or an official document such as a contract or policy. If your company is not showing up in this list, please contact api@support.xero.com

Response

1.2 What is your email address? (If not correct)

Please include the full email address required to complete the assessment. This ensures your contact details are up to date.

Response

1.3 Do you have any additional email addresses that you would like to have included in future assessments?

Please include the other email addresses required to complete the assessment to ensure our contact details are up-to-date.

Note: For entries with more than one email address, please enter in a new line, for example:

- *test@email.com*
- *test2@email.com*

Response

1.4 If any follow up tasks are created due to the result of this assessment, what email address should we send the tasks to?

Response

1.5 Can you help us understand how your application uses the Xero API?

This helps the Xero Security Team, who review this assessment, understand which questions may or may not be applicable to you and focus our security review on the most important areas.

You can talk about how you leverage the Xero API, the purpose it serves, the data being used, and any integrations into your applications.

Response

Section 2 Encryption

2.1 Ensure effective key management is implemented to protect client data.

To meet the requirements for OAuth token management, you must:

- *use OAuth 2.0.*
- *not expose OAuth tokens or customer-identifying information within your application or share them with other parties.*

Response

2.2 Do you encrypt and store any refresh tokens in persistent memory?
Response (Yes/No/Not Applicable)

2.3 Do you encrypt refresh tokens using a symmetric encryption algorithm with a key size of 128 bits or greater?
Response (Yes/No/Not Applicable)

2.4 Do you store your encryption token(s) in a key management service, secret storage service, environment variable, or a separate configuration file?
Response (Yes/No/Not Applicable)

2.5 Ensure that sensitive client data in your app is protected during the transport process. Using TLS 1.2 or higher with strong encryption (AES-256 and SHA-256)
Response

2.6 Does your application server use SSL to support TLS version 1.2 or greater, and use AES-256 or higher with SHA-256 for encryption?
Response (Yes/No/Not Applicable)

2.7 Do your web application endpoints prevent sensitive data or authentication tokens in URL parameters, from appearing in HTML responses?
Response (Yes/No/Not Applicable)

2.8 Ensure that sensitive client data in your application 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.*

Response

2.9 Do you enforce encryption at rest for data repositories containing sensitive commercial or personal information?
Response (Yes/No/Not Applicable)

2.10 Which encryption methods are you using to encrypt data repositories that hold or manage sensitive commercial or personal information?
Response (Full Disk Encryption/Container Encryption/Application Level Encryption/Database Level Encryption)

Section 3 Authentication

3.1 Ensure that users who access your app are authenticated.

Ensure that strong customer authentication is enabled (minimum two step authentication or single sign on). Use of Sign in with Xero is strongly recommended.

Response

3.2 Do you enforce multi factor authentication or single sign-on for all users of your app that are connected to Xero?

Response (Yes/No)

Section 4 Data Hosting & Third-party Access to Data

4.1 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.

Response

4.2 In which country or jurisdiction is your data hosted in?

Response

4.3 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 needs may include (but are not limited to) the utilisation of third party services, which is functionally required. For example, the use of third party biometric services.*

Response

4.4 Do you allow any third party access to customer data (e.g. through an external API or data held)?

Response (Yes/No)

4.5 Is third party access to customer data clearly stated in your policies and or terms and conditions?

Response (Yes/No)

4.6 Please provide a business justification for third party access to customer data

Response

Section 5 Application Server Configuration

5.1 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
- Centre for Internet Security Benchmarks List
- Relevant vendor recommendations

Response

5.2 Do you follow any industry-accepted hardening standards to configure your applications' server?
NOTE: *If you have selected "Do not use a Standard", please provide justification for why you do not need to follow industry-accepted hardening standards.*
Response (CIS/NIST/Vendor Specific/Do not use a Standard)

5.3 Please provide a link to the vendor specific server hardening standard that you use below:
Response

Section 6 Vulnerability Management

6.1 Ensure that your app is secure against common vulnerabilities.
Follow an industry accepted standard for secure code development such as OWASP Top 10 to protect against vulnerabilities
Response

6.2 Which industry accepted standard for secure code development do you use to protect your application against vulnerabilities?
NOTE: *If you have selected "Do not use a Standard", please provide justification for why you do not need to follow industry accepted secure code development standards.*
Response (OWASP Top 10/SANS/CWE Top 25/Other/Do not use a Standard)

6.3 Did you perform any vulnerability scans or assessments in the past 12 months?
Response (Yes/No)

6.4 Were all identified high or critical vulnerabilities remediated?
Response (Yes/No)

Section 7 Security Logging

7.1 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.
Response

7.2 Which attributes do your record logs include?
If you have selected "None of the above", please provide your justification for why you do not log your events.
Response (Application Level (access logs)/Date and Time of the event/Relevant user or Process IDs/Event Description/Success or Failure of the Event/Event Based Actions/ICT Equipment Location and Identification/Event Source e.g. Application Name/None of the above)

7.3 Which of these requirements do you meet as a part of your effective logging strategy?
If you have selected "None of the above", please provide justification as to why you do not have any logging.
Response (Maintain effective logging functionality./Retain logs for a minimum of one year./Retain audit logs for extended periods (e.g., for investigations) as needed./Protect logs from unauthorised modification and deletion/None of the above)

Section 8 Security Monitoring Practices & Incident Lookback

8.1 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 Xero, providing enough information to enable further monitoring and/or preventative action.*

Response

8.2 At what layers do you scan your environment for threats?
Unsure? Hover over each selection to get an example of what scanning at these layers looks like.
If you have selected "None of the above", please provide justification for why you do not scan your environment.
Response (Application layer/Network layer/Infrastructure layer/Transaction (data) layer/None of the above)

8.3 Have you had any security incidents over the past three years?
If yes, please provide high level details about:

- *What the incident was and who was involved*
- *Investigation findings if any*
- *Any controls put in place to lower the likelihood and impact of an incident happening again*

Response (Yes/No)

8.4 Are we confident that the security incident's root cause is fully resolved?
Response (Yes/No)

Section 9 Feedback and Submission

9.1 Thank you for completing the assessment!

We need your help

We recently made some changes to this assessment, such as adding helpful hints for questions, reviewing and updating the question set, improving readability and flow of the assessment and would like to do more. If you could make one change to make this assessment better, what would it be?

Submission:

- *Please check you have completed all questions.*
- *Any questions you have missed will be marked with a 'red star' on the left hand side navigation column.*
- *Once complete, please click on the 'Submit' button.*

Response