🔐

Security Policy

Secoda is committed to security and focused on keeping you and your data safe. Secoda adheres to industry-leading standards while connecting and loading data from all of your data sources.

Contact hello@secoda.co f you have any questions or comments.

Web portal connectivity

- All connections to Secoda's web portal are encrypted by default using industry-standard cryptographic protocols (TLS 1.2+).
- Any attempt to connect over an unencrypted channel (HTTP) is redirected to an encrypted channel (HTTPS).
- To take advantage of HTTPS, your browser must support encryption protection (all versions of Google Chrome, Firefox, and Safari).

Permissions

- **Databases and API cloud applications** - Secoda only requires READ permissions. For data sources that by default grant permissions beyond read-only, Secoda will never make use of those permissions.

Retention of customer data

All customer data, besides what is listed below, is removed from Secoda's system within 24 hours using object lifecycle management. Secoda retains subsets of a customer's data that are required to provide and maintain Secoda's solution. This includes only:

- **Customer access credentials** - Secoda retains customer database credentials and SaaS OAuth tokens in order to securely and continuously extract data and troubleshoot customer issues. These credentials are stored securely using industry standard encryption.

- **Customer metadata** - Secoda retains metadata such as table and column names for each integration so that this information can be shown to your organization in Secoda' user interface.

Physical and environmental safeguards

Since Secoda relies on AWS, physical and environmental security is handled entirely by Amazon. Amazon provides an extensive list of compliance and regulatory assurances, including SOC 1/2-3, PCI-DSS and ISO27001.

Your organization permissions

- Users can use Single Sign-On through Google or Microsoft Apps.
- Only users of your organization registered within Secoda and Secoda operations staff have access to your organization's Secoda workspace.
- Your organization's Secoda workspace provides visibility into the status of each integration, the aforementioned metadata for each integration, and the ability to pause or delete the integration connection - **not organization data.**
- Organization administrators can request that Secoda revoke an organization member's access at any point; these requests will be honored within 24 hours or less.
- Organizations administrators can request that Secoda delete all organizations metadata at any point; these requests will be honoured without 24 hours or less.

Company policies

- Secoda requires that all employees comply with security policies designed to keep any and all customer information safe, and address multiple security compliance standards, rules and regulations.
- Security policies and procedures are documented and reviewed on a regular basis.

- Current and future development follows industry-standard secure coding guidelines, such as those recommended by OWASP.
- Networks are strictly segregated according to security level. Modern, restrictive firewalls protect all connections between networks.

Compliance and privacy

- Secoda currently has SOC 2 compliance and can provide documentation upon request.

In the event of a data breach

To date, Secoda has not experienced a breach in security of any kind. In the event of such an occurrence, Secoda protocol is such that customers would be made aware as soon as the compromise is confirmed.

Responsible disclosure policy

At Secoda, we are committed to keeping our systems, data and product(s) secure. Despite the measures we take, security vulnerabilities will always be possible.

If you believe you’ve found a security vulnerability, please send it to us by emailing hello@secoda.co. Please include the following details with your report:

- Description of the location and potential impact of the vulnerability
- A detailed description of the steps required to reproduce the vulnerability (POC scripts, screenshots, and compressed screen captures are all helpful to us)

Please make a good faith effort to avoid privacy violations as well as destruction, interruption or segregation of services and/or data. We will respond to your report within 5 business days of receipt and will attempt to keep you regularly informed of our progress toward resolving the vulnerability. If you have followed the above instructions, we will not take any legal action against you regarding the report.

Diagnostic data access

> IMPORTANT: Secoda cannot access your data without your approval.

When working on a support ticket, we may need to access your data to troubleshoot or fix your broken connector or destination. In that case, we will ask you to grant Secoda access to your data for the next 21 days. You can allow or deny data access. If you grant us data access, you can revoke it at any moment before the 21-day diagnostic period has expired.