

SAMPLE

Security Questionnaire Response Kit

The opening of SQ-Answer-Library.docx, one of 5 files in the kit. <https://solasai.net/products/security-questionnaire-kit/>

SECURITY QUESTIONNAIRE ANSWER LIBRARY

85 Pre-Drafted Answers for SIG, CAIQ, and Enterprise Questionnaires

Product: *Security Questionnaire Response Kit*

Version: 1.0

Classification: *Purchaser Use Only — Customize Before Use*

Solas AI

solasai.net

Less grind. More growth.

Contents

How to Use This Library

1. Access Control & Identity Management (10 answers)
2. Data Protection & Privacy (10 answers)
3. Network Security (5 answers)
4. Application Security (6 answers)
5. Incident Response (5 answers)
6. Business Continuity & Disaster Recovery (5 answers)
7. Vendor & Third-Party Management (4 answers)
8. Human Resources Security (4 answers)
9. Physical Security (3 answers)
10. Cloud Security (4 answers)

11. Compliance & Governance (5 answers)

12. Privacy & Data Subject Rights (4 answers)

13. AI Security 🤖 (20 answers)

How to Use This Library

This library contains 85 pre-drafted answers organized by security domain. When you receive a questionnaire, find the matching domain, locate the relevant question, and customize the bracketed placeholders with your specific information.

Each answer includes an evidence reference — the artifact you should have ready to support your answer. If you do not have the evidence, your answer should reflect that honestly (see the Response Process Guide for handling gaps).

Customization Required

Every [bracketed placeholder] must be replaced with your company-specific information. Answers are written in first-person organizational voice ("[Company Name] maintains..."). Review each answer against your actual environment before submitting — do not submit answers describing controls you have not implemented.

AI Security Section

Section 13 contains 20 AI-specific answers that most answer libraries do not include. These cover the questions that enterprise security reviewers are increasingly asking AI companies. If you only customize one section, start here.

1. Access Control & Identity Management

Framework mapping: SIG Domain A / CAIQ IAM

AC-01 Do you enforce multi-factor authentication (MFA) for all users?

[Company Name] enforces MFA for all user accounts via [IdP — e.g., Okta, Google Workspace, Entra ID]. MFA is required, not optional — users cannot bypass it. MFA is enforced for both interactive logins and administrative access to cloud infrastructure.

Evidence: *IdP MFA enforcement screenshot*

AC-02 Do you support single sign-on (SSO)?

[Company Name] supports SSO via [SAML 2.0 / OIDC] through [IdP]. Enterprise customers can integrate their own IdP for federated authentication.

Evidence: *SSO configuration documentation*

AC-03 How do you manage user access and permissions?

[Company Name] implements role-based access control (RBAC). Access is granted based on job function and follows the principle of least privilege. Access requests require manager approval and are documented in [ticketing system].

Evidence: *RBAC policy, access request records*

AC-04 How often do you conduct access reviews?

Access reviews are conducted quarterly by [IT / Security Lead]. Reviews verify that access levels remain appropriate for current job functions. Excess access is revoked within 5 business days of review.

Evidence: *Most recent access review record*

AC-05 How is access revoked when an employee leaves?

Access is revoked within 24 hours of employment termination. For involuntary terminations, access is revoked immediately before the individual leaves. Our offboarding checklist covers all systems including cloud infrastructure, SaaS applications, and API credentials.

Evidence: *Offboarding checklist, sample revocation record*

AC-06 Do you manage privileged access separately?

Privileged access (admin roles, production infrastructure) is restricted to designated personnel, requires additional approval from [Security Lead], and is reviewed quarterly. We do not use shared admin accounts.

Evidence: *Privileged access inventory*

AC-07 How are API keys and secrets managed?

API keys and secrets are stored in [secrets management system — e.g., AWS Secrets Manager, HashiCorp Vault]. Secrets are never stored in source code, configuration files, or environment variables in repositories. API keys are rotated on a defined schedule.

Evidence: *Secrets manager configuration, rotation log*

AC-08 Do you support customer-managed SSO?

[Company Name] supports customer SSO integration via [SAML 2.0 / OIDC]. Enterprise customers can configure their own identity provider for authentication, maintaining control over user provisioning and deprovisioning.

Evidence: *SSO integration documentation*

AC-09 How do you handle session management?

User sessions expire after [timeout period] of inactivity. Sessions are invalidated on password change. Concurrent session limits are enforced at [number] per user. Session tokens are transmitted only over encrypted connections.

The sample ends here. The full document runs about 4,411 words; the kit holds 5 files. Version 2.2, 19 October 2026. Buy it at <https://solasai.net/products/security-questionnaire-kit/>, 14-day refund for any reason.