



The 113 Most Commonly-Asked Security Questions


A Helpful List for Security and GRC Leaders

At SafeBase, we've helped hundreds of customers populate their Smart Trust Centers, build out Knowledge Bases, and fill out security questionnaires. These are the top 113 (yes, 113!) security questions that we see most frequently.

The list of questions covers topics including:

- Policies
- Business Information
- Cryptography Standards
- Security Tools
- Security & Privacy Compliance
- Application Security

We recommend answering all of these questions and having them on hand - or even, better, available in your SafeBase Knowledge Base.



Question
Name of the holding or parent company
Company/business name
HQ Address
Publicly or privately held company
If public, what is the name of the Exchange?
If public, what is the trading symbol?
Type of legal entity and state of incorporation
How long has the company been in business?
Description of service/product being provided.
Are you considered a processor or controller?
Does your application provide an API?
What's the session timeout? Is this configurable?
Describe the application's tech stack.
Explain the data flow.
Name the organization's Cloud Service Provider (CSP).
Name the organization's Cloud locations (including backup/recovery site).
Please list services provided to you by the Cloud Service Provider (CSP). Examples include KMS, backup, data recovery.
Please provide an explanation of the data center's Physical security or provide a link.
How do you train developers in SSDLC / Secure Coding Practices?
Describe the Software Development Lifecycle (SDLC).
Describe access to the dev environment.
Is production data used in non-production environments? If so, is it anonymized or pseudonomized?
Describe the internal authentication method used by the organization.
Describe the external authentication method used by the organization.
Describe certificate-based authentication used by the organization.
Describe the method used for data in-transit.
Describe the method used for data at rest.
What is the name of the KMS provider? Please include details.
Is background screening a part of the hiring process and what does that include?
Are employees required to attend security awareness training?
Are employees required to attend privacy training?
Do you perform pen testing of the web application? If so, what is the frequency?
Do you perform pen testing of the network? If so, what is the frequency?
Do you perform pen testing of the infrastructure? If so, what is the frequency?
What is the tool utilized to conduct vulnerability scans?
Are vulnerability scans conducted both internally and externally?
What is the frequency of vulnerability scans?
Is a SIEM utilized? If so, who is the software provider?

Does the organization log and audit logs for the following events: unsuccessful login attempts, successful login attempts, privilege escalation, account creation, password changes, and unrecognized processes? If not all event types are logged, please elaborate.
Describe the physical security of the office, if applicable.
Describe the physical security of the data center or provide a link to the security page of the Cloud Service Provider.
Does your organization use IDS/IPS tools?
Does your organization use firewalls?
Does your organization use DLP?
Who is your MDM provider?
Are anti-malware and anti-virus detection and prevention technology services configured on managed endpoints?
Describe provisioning/de-provisioning procedures.
Describe remote access.
Describe log access.
List data types needed to provide services.
Describe any data retention procedures/policies.
Describe any data disposal procedures/policies.
Describe the process for breach notifications.
Describe the process for a security/privacy concern.
Do you have anyone responsible for Data Privacy compliance (This could be a Data Protection Officer, Chief Privacy Officer, General Counsel etc.)? If yes, please provide contact information.
Will data be processed or transferred outside of the US?
Was your organization affected by the SolarWinds vulnerability/breach?
Was your organization affected by the Atlassian vulnerability/breach?
Was your organization affected by the Accellion vulnerability/breach?
Was your organization affected by the Log4j vulnerability/breach?
Was your organization affected by the Okta vulnerability/breach?
Is your organization compliant with GDPR?
Is your organization compliant with HIPAA?
Is your organization compliant with PIPEDA?
Is your organization compliant with CCPA?
Is your organization compliant with CSA STAR?
Is your organization compliant with Privacy Shield?
Is your organization compliant with SOC 2?
Is your organization compliant with ISO 27001?
Please provide the organization's Public URL.
Please provide the organization's Status Page (Live Uptime).
Please provide the organization's API Documentation.
Please provide the organization's Privacy Policy.
Please provide the organization's Cookie Policy.

Please provide the organization's Trust Center URL.
Please provide the organization's Terms of Service/Legal Page.
Please provide the organization's Subprocessors List.
Does your organization have an MSA?
Does your organization have a DPA?
Does your organization have an SLA?
Does your organization have a TOS?
Has your organization completed a SIG questionnaire?
Has your organization completed a SIG Lite questionnaire?
Has your organization completed a SIG Core questionnaire?
Has your organization completed a CAIQ questionnaire?
Has your organization completed a CAIQ Lite questionnaire?
Has your organization completed a VSA questionnaire?
Has your organization completed a VSA Full questionnaire?
Has your organization completed a HECVAT questionnaire?
Has your organization completed a HECVAT Lite questionnaire?
Does your organization have an Acceptable Use Policy?
Does your organization have an Access Control Policy?
Does your organization have an Anti-Malicious Software Policy?
Does your organization have an Asset Management Policy?
Does your organization have a Backup Policy?
Does your organization have a Business Continuity Policy?
Does your organization have a BYOD Policy?
Does your organization have an Internal and External Communication Policy?
Does your organization have a Data Classification Policy?
Does your organization have a Data Sanitization Policy?
Does your organization have a Data Security Policy?
Does your organization have an Encryption Policy?
Does your organization have an IMS Policy?
Does your organization have a General Incident Response Policy?
Does your organization have an Information Security Policy?
Does your organization have a Network Security Policy?
Does your organization have a Password Policy?
Does your organization have a Physical Security Policy?
Does your organization have a Risk Management Policy?
Does your organization have a Software Development Lifecycle Policy?
Does your organization have a Third-Party Personnel Policy?
Does your organization have a Vulnerability and Patch Management Policy?