VendorClerk

Google VSAQ: security & privacy program + web application

Sample draft for **Brambleway, Inc.** (fictional), a 31-person HR onboarding SaaS company.

Fictional sample. Brambleway, Inc. is a fictional company. Its policy pack was written by VendorClerk for this demonstration, and the answers below were drafted by VendorClerk's engine from that pack only. Nothing here describes a real organization.

62 questions	**41** ready to review (High confidence, cited)
15 drafted, with a follow-up question for you	**6** left blank and flagged (not in the docs)

Every answer cites the document section it came from. High fully supported Medium mostly supported, please confirm Low not supported, so we ask instead of guessing.

ID	Question	Draft answer	Confidence / what we need
SP-01	Security and Privacy Does your company have a strong, established security program, and does the scope of the program include all information processed as part of this project?	Yes, our security program covers all aspects of information security for this project. Source: information_security_policy.md > 1. Scope and governance; information_security_policy.md > 2. Policy topics; trust_overview.md > Compliance	Medium **We ask you:** Please confirm that all information processed for this project is customer data on the HR onboarding platform already in program scope, and that you are comfortable attesting the program covers all aspects of information security for the project.
SP-02	Security and Privacy > Security and Privacy Program Details Standards and guidelines are available for security and privacy programs. Complying with a generally accepted standard helps your customers assess the controls and safeguards that make up your program. Examples of standards include ISO 27001 , PCI DSS , and SSAE 16 . Which option applies?	Our security program is based on a recognized security standard, and it can easily be audited against that. Source: information_security_policy.md > 1. Scope and governance; trust_overview.md > Compliance	High
SP-03	Security and Privacy > Security and Privacy Program Details What's the name of the standard or set of best practices that your security program is based on?	Brambleway's security program is aligned with the AICPA SOC 2 Trust Services Criteria and uses the CIS Controls v8 as an implementation guide. Source: information_security_policy.md > 1. Scope and governance	High
SP-04	Security and Privacy > Security and Privacy Program Details Does your information security and privacy program cover all of your operations, services, and systems that involve access to confidential information?	Yes, both the processes that directly deal with customer data (such as IT) and the processes that might indirectly affect the security of customer data (such as HR processes) are in scope. Source: information_security_policy.md > 1. Scope and governance; information_security_policy.md > 2. Policy topics; information_security_policy.md > 15. Human resources security	High

ID	Question	Draft answer	Confidence / what we need
SP-05	Security and Privacy > Security and Privacy Program Details Has your company selected an individual or team to be responsible for managing the information security and privacy program?	Yes, management has selected an individual or team to be responsible for the information security and privacy program. Source: information_security_policy.md > 1. Scope and governance; information_security_policy.md > Brambleway, Inc. Information Security Policy (FICTIONAL SAMPLE)	High
SP-06	Security and Privacy > Security and Privacy Program Details How many employees in the company spend more than 50% of their time working on information security?	One employee spends more than 50% of their time on information security. We have one full-time security engineer who spends 100% of their time on information security; our VP of Engineering spends roughly a third of their time on it. Source: information_security_policy.md > 1. Scope and governance	High
SP-07	Security and Privacy > Security Controls Select the controls you currently maintain as elements of your information security and privacy program:	Written internal policies, guidelines, and documented practices for the safe handling and protection of data | Internal audits of the security and privacy program | Third-party audits of the security and privacy program | A program to ensure security in your human resources processes | Processes and procedures to ensure that security incidents are discovered in a timely manner and dealt with effectively Source: information_security_policy.md > 2. Policy topics; information_security_policy.md > 4. Internal and external assessment; information_security_policy.md > 15. Human resources security; information_security_policy.md > 12. Incident response	Medium **We ask you:** Please confirm whether you publish an external policy or notice to the public, users, or customers describing how you protect data, and whether you maintain a risk assessment process that regularly reviews threats to the company. Please also confirm whether vendor and subprocessor management verifies that providers can protect sensitive data and systems, whether change management reviews all changes to networks, systems, and processes, and whether incidents are discovered in a timely manner.
SP-08	Security and Privacy > Security Controls Provide a link to your public security and/or privacy policy.	We publish our privacy notice at brambleway.example/privacy. Source: information_security_policy.md > 18. Data retention, deletion, and privacy	High

ID	Question	Draft answer	Confidence / what we need
SP-09	Security and Privacy > Security and Privacy Policies Select the topics that are covered by your security and privacy policies:	Information classification and protection | Security in human resources | Physical security requirements | Acceptable use of information and IT devices | Access control | Software development | Incident management and response procedures for both security and privacy incidents | Compliance with laws and regulations | Retention and destruction of data Source: information_security_policy.md > 2. Policy topics	Medium **We ask you:** Please confirm whether your security and privacy policies explicitly cover authorized and unauthorized use and disclosure of data. If they do, provide the policy or section name so we can include that topic.
SP-10	Security and Privacy > Security and Privacy Policies How often does your company review its security and privacy policies to ensure they are up to date?	Once per year. Source: information_security_policy.md > Brambleway, Inc. Information Security Policy (FICTIONAL SAMPLE)	Medium **We ask you:** The policy is reviewed at least once per year and also whenever a significant change occurs, but the evidence does not say those change-driven reviews happen immediately or multiple times per year. Please confirm we should select “Once per year,” or specify which single choice you want.
SP-11	Security and Privacy > Internal Assessments How often are internal information security and privacy audits performed?	Quarterly or more often. Source: information_security_policy.md > 4. Internal and external assessment	High
SP-12	Security and Privacy > Internal Assessments Does the scope of your internal assessment include the entire security and privacy program, as well as all operations, services, and systems that involve access to the customer data or systems that are used in this project?	*Left blank: not covered by the documents*	Low **We ask you:** Please confirm whether the quarterly internal assessment covers the entire security and privacy program and all operations, services, and systems that involve access to customer data or are used in this project. The policy only states that it covers all systems that store or process customer data against the SOC 2 control set.

ID	Question	Draft answer	Confidence / what we need
SP-13	Security and Privacy > Internal Assessments How is the scope limited?	We scope quarterly internal control assessments to the SOC 2 control set and to all systems that store or process customer data. Source: information_security_policy.md > 4. Internal and external assessment	High
SP-14	Security and Privacy > Internal Assessments Does your internal assessment audit your company's compliance with any specific information security or privacy standards?	Yes. Source: information_security_policy.md > 4. Internal and external assessment	High
SP-15	Security and Privacy > Internal Assessments To what standards does your internal assessment audit compliance?	Our internal control assessment audits compliance against the SOC 2 control set. Source: information_security_policy.md > 4. Internal and external assessment	High
SP-16	Security and Privacy > Third-Party Audits How often does an independent third party perform audits of your security and privacy program?	Annually. Source: information_security_policy.md > 4. Internal and external assessment; trust_overview.md > Compliance	High
SP-17	Security and Privacy > Third-Party Audits Does the scope of these third party audits include the entire security and privacy program, as well as all operations, services, and systems that involve access to sensitive information or systems?	*Left blank: not covered by the documents*	Low **We ask you:** Please confirm whether the scope of the annual SOC 2 Type II examination and third-party penetration test includes the entire security and privacy program and all operations, services, and systems that involve access to sensitive information or systems, or whether those audits are limited.

ID	Question	Draft answer	Confidence / what we need
SP-18	Security and Privacy > Third-Party Audits Describe the limits of these external audits:	An independent CPA firm performs a SOC 2 Type II examination every year. We are not ISO 27001 certified. Customers under NDA may request the full SOC 2 Type II report; a management summary is available on request. Source: information_security_policy.md > 4. Internal and external assessment; information_security_policy.md > 1. Scope and governance	Medium **We ask you:** Please confirm the SOC 2 Type II report period, in-scope systems and Trust Services Criteria, and any stated limitations, carve-outs, or exceptions. Also confirm whether any external audits besides the annual SOC 2 Type II should be described.
SP-19	Security and Privacy > Third-Party Audits Does the independent audit including checking your company's compliance with any specific information security or privacy standard?	Yes. Source: trust_overview.md > Compliance; information_security_policy.md > 4. Internal and external assessment	High
SP-20	Security and Privacy > Third-Party Audits What standards does the audit comply with?	Our annual independent third-party audit is a SOC 2 Type II examination aligned with the AICPA SOC 2 Trust Services Criteria. Source: information_security_policy.md > 4. Internal and external assessment; information_security_policy.md > 1. Scope and governance	High
SP-21	Security and Privacy > Third-Party Audits Describe how you select auditors and how often you change auditors, and list the auditors you selected for the three most recent audits:	We select auditors through a competitive proposal process and review the auditor relationship every three years. Source: information_security_policy.md > 4. Internal and external assessment	Medium **We ask you:** Please confirm how often you change auditors (the relationship is reviewed every three years, but a change cycle is not stated) and list the auditors selected for the three most recent audits.
SP-22	Security and Privacy > Third-Party Audits Are you willing to share a management summary of the most recent audit reports?	Yes. Source: information_security_policy.md > 4. Internal and external assessment	High

ID	Question	Draft answer	Confidence / what we need
SP-23	Security and Privacy > Risk Assessment/Risk Management Under your risk management process, how often are risk assessments reviewed and updated?	Multiple times per year. Source: information_security_policy.md > 3. Risk management	High
SP-24	Security and Privacy > Partner Security Program Has your company selected an individual or team to be responsible for reviewing service providers and subcontractors, to ensure that they sufficiently protect the security and privacy of sensitive information and systems?	Yes. Source: information_security_policy.md > 14. Vendor and subprocessor management	High
SP-25	Security and Privacy > Partner Security Program Do your written contracts with relevant third parties require them to adequately protect the privacy and security of all confidential information they may get access to during the partnership?	*Left blank: not covered by the documents*	Low **We ask you:** Please confirm whether written contracts with all outsourcing providers, vendors, and subcontractors that may access confidential information—not only subprocessors—require them to protect privacy and security. We can select the Yes choice only if that broader coverage is confirmed; otherwise the No choice may apply.
SP-26	Security and Privacy > Change Management Is your change management process formally documented, and does it classify changes by impact and size?	Our change management process is documented in the engineering handbook and classifies changes as standard, normal, or emergency according to impact. Source: information_security_policy.md > 11. Change management and secure development	Medium **We ask you:** Please confirm whether the change management process also classifies changes by size, and if so which size categories are used.

ID	Question	Draft answer	Confidence / what we need
SP-27	Security and Privacy > Change Management Does your change review board include representatives from the teams that are responsible for security and privacy?	*Left blank: not covered by the documents*	Low **We ask you:** The security engineer sits on the weekly change review. Please confirm whether that change review board also includes a representative responsible for privacy, so we can answer Yes or No.
SP-28	Security and Privacy > Change Management Do you retain records and documentation about the changes that go through change management?	Yes. We retain pull request history, approvals, and deployment records for changes that go through change management for at least three years. Source: information_security_policy.md > 11. Change management and secure development	High
SP-29	Security and Privacy > Security and Privacy Incident Response Select the controls you have in place for identifying security and privacy incidents as quickly as possible:	*Left blank: not covered by the documents*	Low **We ask you:** Please confirm which controls are in place to identify security and privacy incidents quickly: signature- and/or anomaly-based IDS/IPS with sensors at strategic network points, regular log-file review for signs of intrusion, and/or other detection methods. If other methods are used, describe them.
SP-30	Security and Privacy > Security and Privacy Incident Response Describe the other detection methods you have in place.	We detect anomalous activity with Amazon GuardDuty and AWS Security Hub, which correlate CloudTrail, VPC Flow Logs, and DNS events in all accounts. Application audit logs alert on unusual sign-in patterns and bulk data exports, and those alerts go to the on-call engineer through PagerDuty 24×7. Endpoint detection and response runs on all company laptops. Source: information_security_policy.md > 9. Logging and monitoring	High

ID	Question	Draft answer	Confidence / what we need
SP-31	Security and Privacy > Security and Privacy Incident Response Are incident response procedures documented?	Yes. We maintain a documented incident response plan covering both security and privacy incidents, with defined roles, severity levels, an escalation path, evidence handling, and customer communication steps. The plan is approved by the CEO, reviewed annually, and communicated to every engineer during on-call onboarding. Source: information_security_policy.md > 12. Incident response	High
SP-32	Security and Privacy > Security and Privacy Incident Response Do you have the resources to internally conduct incident investigations?	Yes. We have internal resources to conduct incident investigations, including a documented incident response plan with defined roles, evidence handling, and a full-time security engineer. An external forensics firm is retained for investigations that exceed internal capacity. Source: information_security_policy.md > 12. Incident response; information_security_policy.md > 1. Scope and governance	High
SP-33	Security and Privacy > Security and Privacy Incident Response Explain how you'll get the necessary resources for incident investigation when you need them:	We engage investigation resources through our documented incident response plan, which defines roles, severity levels, and an escalation path. When an investigation exceeds internal capacity, we use our incident response retainer with an external forensics firm. Source: information_security_policy.md > 12. Incident response	High

ID	Question	Draft answer	Confidence / what we need
SP-34	Security and Privacy > Security and Privacy Incident Response Do you inform affected customers about security incidents?	Yes. We notify affected customers without undue delay, and in any case within 72 hours of confirming a security incident that affects their data, as committed in our Data Processing Addendum. Our incident response plan includes customer communication steps. Source: information_security_policy.md > 12. Incident response	High
SP-35	Security and Privacy > Personnel Security Do you have written job descriptions for employees with access to confidential or sensitive information?	Yes. Every role with access to Confidential or Customer Data has a written job description that defines its security responsibilities. Source: information_security_policy.md > 15. Human resources security	High
SP-36	Security and Privacy > Personnel Security Do you have processes in place to ensure that access to data is granted solely on a "need-to-know" basis, in accordance with the job descriptions and responsibilities of users? Do these processes also revoke access when the need no longer exists?	Yes. We grant access on a least-privilege, need-to-know basis according to each person's role, and every role with access to Confidential or Customer Data has a written job description defining its security responsibilities. Access requests are approved by the employee's manager and the Security Lead. We disable access within four hours of termination, review access within five business days of a role change, and revalidate least privilege quarterly. Source: information_security_policy.md > 6. Access control; information_security_policy.md > 15. Human resources security	High
SP-37	Security and Privacy > Personnel Security Do you have a disciplinary process in place for handling policy violations?	Yes. We handle violations of security policy through a documented disciplinary process that can lead to termination. Source: information_security_policy.md > 15. Human resources security	High

ID	Question	Draft answer	Confidence / what we need
SP-38	Security and Privacy > Personnel Security Do you have processes in place to make sure access (both physical and logical) is revoked when an employee, intern, vendor, contractor, or other associate leaves the company or a contract ends?	*Left blank: not covered by the documents*	Low **We ask you:** Please confirm whether physical facility access, such as badges, keys, or office entry, is revoked when someone leaves and within what timeframe. Also confirm the same revocation process covers interns, vendors, contractors, and other associates when they leave or a contract ends.
SP-39	Security and Privacy > Personnel Security How often do you require your employees to undergo information security and privacy training?	Upon hire, and at least once per year. Source: information_security_policy.md > 15. Human resources security	High
SP-40	Security and Privacy > Personnel Security Do you require temps, interns, and contractors to undergo security and privacy training?	Yes. We require contractors to complete security and privacy awareness training at onboarding and annually. Interns and temporary staff complete the same training before receiving access. Source: information_security_policy.md > 15. Human resources security	High
SP-41	Security and Privacy > Personnel Security Do you perform background checks for personnel who are entrusted with sensitive information or granted access to sensitive systems?	Yes. We perform criminal background checks and employment verification for United States employees before their start date, as permitted by law. Contractors with production access undergo the same checks. Source: information_security_policy.md > 15. Human resources security	High

ID	Question	Draft answer	Confidence / what we need
SP-42	Security and Privacy > Personnel Security > Background Checks What kinds of background checks do you perform for employees who potentially have access to confidential information?	Criminal record/conviction checks | Other background checks, as described below Source: information_security_policy.md > 15. Human resources security	High
SP-43	Security and Privacy > Personnel Security > Background Checks Describe the other checks you perform for new hires:	Brambleway employees in the United States undergo a criminal background check and employment verification before their start date, as permitted by law. Contractors with production access undergo the same checks. Source: information_security_policy.md > 15. Human resources security	Medium **We ask you:** Please confirm that criminal background checks and employment verification for United States employees and production-access contractors are the checks to report, and supply any other checks for new hires, including employees outside the United States.
SP-44	Security and Privacy Is there anything else you want us to know about your security program?	The VP of Engineering is accountable for our security and privacy program and reports security metrics and open risks to the CEO and board quarterly. We align with SOC 2 Trust Services Criteria and use CIS Controls v8; we are not ISO 27001 certified. One full-time security engineer spends 100% of their time on information security, and we perform an annual independent penetration test plus a public vulnerability disclosure program. Source: information_security_policy.md > 1. Scope and governance; information_security_policy.md > 10. Vulnerability management and penetration testing	High

ID	Question	Draft answer	Confidence / what we need
WA-01	Application > Vulnerability Reporting and Management Do you have an easily discoverable way for external researchers to report security vulnerabilities in your systems?	Yes, we have a published security email contact, or we provide another way for users to report security issues. Incoming reports are timely reviewed and triaged. Source: trust_overview.md > Security contacts; information_security_policy.md > 10. Vulnerability management and penetration testing	Medium **We ask you:** Please confirm that incoming vulnerability reports are reviewed and triaged, not only acknowledged within two business days.
WA-02	Application > HTTPS and Mixed-Content Risks > Configuring SSL/TLS Have you recently reviewed your SSL configuration to ensure that only secure protocols and ciphers are offered to clients?	Yes, we regularly review the cipher suite advertised by the server and the protocols it uses. Source: application_security.md > TLS configuration	High
WA-03	Application > HTTPS and Mixed-Content Risks > Configuring SSL/TLS Does your server offer forward secrecy for clients that support it?	We terminate TLS at the AWS Application Load Balancer using the ELBSecurityPolicy-TLS13-1-2-2021-06 policy, which allows only TLS 1.2 and TLS 1.3 with forward-secret ECDHE cipher suites. Clients that support these suites receive forward secrecy. Source: application_security.md > TLS configuration	Medium **We ask you:** Please confirm whether DHE cipher suites are also enabled. The Yes choice requires both ECDHE and DHE, and current TLS configuration only documents forward-secret ECDHE cipher suites on ELBSecurityPolicy-TLS13-1-2-2021-06.
WA-04	Application > HTTPS and Mixed-Content Risks > Configuring SSL/TLS Are your SSL/TLS private keys appropriately protected on your web servers?	Yes, we have taken all necessary steps to protect our private keys. Source: application_security.md > TLS configuration	High
WA-05	Application > Authentication and Authorization > Username/Password Authentication Does the application enforce minimum password security requirements (e.g., a certain length, character classes, etc.)?	Yes. We require passwords of at least 12 characters and check them against a breached-password list. We do not enforce character-class composition rules. Source: application_security.md > Authentication	High

ID	Question	Draft answer	Confidence / what we need
WA-06	Application > Authentication and Authorization > Username/Password Authentication > Password Storage How does the application store passwords?	Using a dedicated password-based key derivation function, such as bcrypt , PBKDF2 or scrypt Source: application_security.md > Authentication	High
WA-07	Application > Authentication and Authorization > Username/Password Authentication > Setting an Initial Password How do users get their initial passwords?	The initial password or a link to set the initial password is sent to users by email. Source: application_security.md > Authentication	Medium **We ask you:** Please confirm the one-time invitation link is sent by email. We can confirm new users set their own password via an expiring invitation link and that we never send initial passwords, but the delivery channel is not stated.
WA-08	Application > Authentication and Authorization > Authentication Cookies and Sessions Cookies can be decorated with a special keyword, HttpOnly . If this keyword is set, the browser will not allow JavaScript to access the cookie. Even if the application has a cross-site scripting vulnerability, this keyword makes it much harder for an attacker to steal the session cookie. Which option applies?	The HttpOnly keyword is set for all our authentication cookies. Source: application_security.md > Sessions	High
WA-09	Application > Authentication and Authorization > Authentication Cookies and Sessions Does your application offer a "log out" button or link that, when clicked, not only terminates the session (deletes cookies from the client) but also invalidates the entire session ID?	Yes. When a user logs out, we invalidate the session on the server, not only in the browser. Source: application_security.md > Sessions	Medium **We ask you:** Please confirm that the application offers a user-facing log out button or link, and that clicking it deletes the session cookie from the client as well as invalidating the session ID on the server.

ID	Question	Draft answer	Confidence / what we need
WA-10	Application > Authentication and Authorization > Authorization Horizontal Access Control : Horizontal access control refers to isolation between users of the same role. For example, consider an application that allows users to access their payroll statements. The application must ensure that a user cannot access another user's statements; i.e., if the user's statement for the month of May is found at statement.html?id=837 2 &month=5 , it shouldn't be possible to see someone else's pay stub simply by loading statement.html?id=837 3 &month=5 . Which option applies?	Our application enforces these restrictions on the server side. We have processes in place to make sure nothing slips through the cracks. Source: application_security.md > Authorization	High
WA-11	Application > Authentication and Authorization > Authorization Vertical Access Control : When an application supports multiple roles, users should not be able to gain privileges or perform unauthorized actions by loading pages or features that should only be available to users in a different role. Throughout your application, have you ensured that users can perform only those actions that are appropriate for their roles?	Our application enforces these restrictions on the server side. We have processes in place to make sure nothing slips through the cracks. Source: application_security.md > Authorization	Medium **We ask you:** Please confirm that a defined process, such as automated tests or reviews, specifically checks vertical role authorization so unauthorized actions cannot be missed. Evidence describes automated tests for tenant isolation, not for role checks.
WA-12	Application > Authentication and Authorization > Authorization-Related Web Vulnerabilities > Cross Site Request Forgery Does your application protect all state-changing actions against XSRF?	Yes, all state-changing actions are protected. Source: application_security.md > Common web vulnerabilities	Medium **We ask you:** Please confirm whether XSRF-token checks are enforced in a central place, or another control ensures no state-changing action can miss XSRF protection, so the full questionnaire option can be selected.

ID	Question	Draft answer	Confidence / what we need
WA-13	Application > Common Web Vulnerabilities > Cross-Site Scripting In addition to applying the strategies you've identified, does the application set a valid and appropriate content type and character set for each page (in the Content-Type HTTP header)?	Yes, we take great care to set this, knowing that otherwise we might be introducing XSS vulnerabilities. Source: application_security.md > Common web vulnerabilities	High
WA-14	Application > Common Web Vulnerabilities > File Uploads Where does the application store those files?	Somewhere else Source: application_security.md > File uploads; application_security.md > Architecture and frameworks	High
WA-15	Application > Common Web Vulnerabilities > File Uploads What types of files does your application white-list?	We whitelist only PDF, JPG, PNG, and HEIC files for onboarding document uploads. Source: application_security.md > File uploads	High
WA-16	Application > Testing, QA, and Monitoring Are you using unit tests or similar methods?	Yes. We maintain automated unit and integration tests with about 85% line coverage, including security-specific tests for authorization, tenant isolation, CSRF, and output escaping. Source: application_security.md > Testing	High
WA-17	Application > Testing, QA, and Monitoring > Unit Testing How would you describe the code coverage of your unit tests?	Robust: The vast majority of our code is tested through unit tests; code coverage is at least >80%. Source: application_security.md > Testing	Medium **We ask you:** Please confirm that unit-test coverage alone is at least 80%, since the stated figure of about 85% line coverage combines unit and integration tests, and provide the latest unit-test-only coverage percentage.
WA-18	Application > Testing, QA, and Monitoring Do your engineers and your QA team look for potential security issues during release testing, and have they been trained to do so?	Yes, our QA process explicitly includes testing for security issues that might have been introduced in the new version. Source: application_security.md > Testing	High

About the questions. Question text from Google's open-source Vendor Security Assessment Questionnaire (github.com/google/vsaq), Apache License 2.0, flattened to a spreadsheet by VendorClerk.
This is the unedited first draft, exactly as our engine produced it, before human QA. In a real order you also get the filled file in its original format and a review sheet listing only the questions that need you.

VendorClerk drafts security questionnaires from your own documents; you review and approve every answer. vendorclerk.com · hello@vendorclerk.com