VendorClerk

SIG Lite-style vendor security assessment

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.

35 questions	**27** ready to review (High confidence, cited)
5 drafted, with a follow-up question for you	**3** 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
GOV-01	GOV Do you have a documented information security policy that is approved by management and reviewed at least annually?	Yes. Brambleway maintains a documented information security policy approved by the CEO on 2026-03-02. We review and re-approve the policy and its supporting procedures at least once per year, and whenever a significant change to the business, infrastructure, or threat landscape occurs. Source: information_security_policy.md > Brambleway, Inc. Information Security Policy (FICTIONAL SAMPLE)	High
GOV-02	GOV Is there a named individual responsible for the information security program?	Yes. Brambleway's VP of Engineering owns the information security program and also acts as the Security Lead. That role is accountable for the information security and privacy program and reports security metrics and open risks to the CEO and the board quarterly. Source: information_security_policy.md > 1. Scope and governance; information_security_policy.md > Brambleway, Inc. Information Security Policy (FICTIONAL SAMPLE)	High
GOV-03	GOV Do you perform a formal risk assessment at least annually?	Yes. We perform a formal information security risk assessment at least annually and whenever a major change is introduced. Risks are recorded in a risk register with an owner, likelihood, impact, and treatment decision. The risk register is reviewed quarterly by the Security Lead and the CEO. Source: information_security_policy.md > 3. Risk management	High
GOV-04	GOV Do you hold a current SOC 2 Type II report? If yes, which trust services criteria are in scope?	Yes. We hold a current SOC 2 Type II report covering the Security, Availability, and Confidentiality Trust Services Criteria for the period 2025-07-01 to 2026-06-30. An independent CPA firm performed the examination, and the report contained no exceptions. Source: trust_overview.md > Compliance; information_security_policy.md > 4. Internal and external assessment	High

ID	Question	Draft answer	Confidence / what we need
GOV-05	GOV Are you ISO 27001 certified?	No. We are not ISO 27001 certified. Our information security program is aligned with the AICPA SOC 2 Trust Services Criteria, and we have completed a SOC 2 Type II examination covering Security, Availability, and Confidentiality with no exceptions. Source: trust_overview.md > Compliance; information_security_policy.md > 1. Scope and governance	High **We ask you:** Please confirm that Brambleway is not ISO 27001 certified, or provide a current certificate if certification status has changed.
GOV-06	GOV Do you carry cyber liability insurance? Please state the coverage amount.	*Left blank: not covered by the documents*	Low **We ask you:** Please confirm whether Brambleway carries cyber liability insurance and, if so, state the coverage amount.
HR-07	HR Are background checks performed on employees prior to hire?	Yes. Employees in the United States undergo a criminal background check and employment verification before their start date, as permitted by law. Source: information_security_policy.md > 15. Human resources security	Medium **We ask you:** Please confirm whether background checks are also completed for employees outside the United States before hire, and whether checks are finished before the hiring decision rather than only before the start date.
HR-08	HR Do all employees complete security awareness training at least annually?	Yes. All Brambleway employees and contractors complete security and privacy awareness training at onboarding and annually, plus quarterly phishing simulations. Interns and temporary staff complete the same training before receiving access. Source: information_security_policy.md > 15. Human resources security	High
HR-09	HR Do employees and contractors sign confidentiality agreements?	Yes. All Brambleway employees and contractors sign confidentiality agreements. Source: information_security_policy.md > 15. Human resources security	High

ID	Question	Draft answer	Confidence / what we need
IAM-10	IAM Is multi-factor authentication enforced for all employee access to production systems?	Yes. We enforce phishing-resistant multi-factor authentication (WebAuthn security keys) for every workforce account, including administrators, through Okta single sign-on. Production AWS access uses AWS IAM Identity Center with short-lived credentials, and humans have no long-lived IAM user access keys. Source: information_security_policy.md > 6. Access control	High
IAM-11	IAM Are user access reviews performed at least quarterly?	Yes. We perform user access reviews for production systems and critical SaaS tools quarterly. Each review revalidates least privilege and checks separation of duties. Source: information_security_policy.md > 6. Access control	High
IAM-12	IAM Is access removed within 24 hours of an employee's termination?	Yes. We disable the Okta account and all downstream access within four hours of termination and remotely lock company laptops. Source: information_security_policy.md > 6. Access control	High
IAM-13	IAM Do you support SAML single sign-on for customer users?	Yes. Customer administrators can require SAML 2.0 single sign-on (Okta, Microsoft Entra ID, or Google Workspace) for their organization. Source: application_security.md > Authentication	High
IAM-14	IAM What is your minimum password length requirement?	We require a minimum password length of 12 characters. Source: application_security.md > Authentication	High

ID	Question	Draft answer	Confidence / what we need
DATA-15	DATA Is customer data encrypted at rest? Describe the algorithm and key management.	Yes. We encrypt customer data at rest with AES-256 using AWS KMS customer-managed keys for Amazon RDS (PostgreSQL), Amazon S3, and EBS volumes. KMS keys rotate automatically every year and immediately if compromise is suspected. Encryption uses AWS-managed cryptographic modules validated under FIPS 140-3. Source: information_security_policy.md > 7. Cryptography and key management	High
DATA-16	DATA Is customer data encrypted in transit using TLS 1.2 or higher?	Yes. We encrypt customer data in transit with TLS 1.2 or higher. TLS terminates at the AWS Application Load Balancer under a policy that permits only TLS 1.2 and TLS 1.3 with forward-secret cipher suites, and traffic between the load balancer and application containers is re-encrypted with TLS inside the VPC. Source: information_security_policy.md > 7. Cryptography and key management; application_security.md > TLS configuration	High
DATA-17	DATA In which countries or regions is customer data stored?	We store all customer data in the United States only, in AWS us-west-2, with backups and a warm standby in AWS us-east-1. Source: trust_overview.md > Hosting and data location	High
DATA-18	DATA Is customer data deleted upon contract termination? Within what time frame?	Yes. On contract termination, we delete Customer Data within 30 days unless the customer requests an export first. Source: information_security_policy.md > 18. Data retention, deletion, and privacy	High
DATA-19	DATA Is customer data used to train AI or machine learning models?	*Left blank: not covered by the documents*	Low **We ask you:** Please confirm whether Brambleway uses customer data to train any AI or machine learning models. If yes, describe the purpose, data used, and any customer controls; if no, confirm so the answer can be No.

ID	Question	Draft answer	Confidence / what we need
INFRA-20	INFRA Where is your production environment hosted?	We host our production environment in AWS us-west-2 (Oregon), with a warm standby in us-east-1. All customer data is stored and processed in the United States. Source: trust_overview.md > Hosting and data location; information_security_policy.md > 8. Network and infrastructure security	High
INFRA-21	INFRA Are production, staging and development environments logically separated?	Yes. We run production, staging, and development in separate AWS accounts under AWS Organizations. Source: information_security_policy.md > 8. Network and infrastructure security	High
APPSEC-22	APPSEC Are all code changes peer reviewed before deployment to production?	Yes. We require every code change to be reviewed and approved by a second engineer through a pull request before merge, with automated tests, static analysis, and dependency scanning. Production deployments run only through our CI/CD pipeline, and engineers cannot deploy from their laptops. Source: information_security_policy.md > 11. Change management and secure development	Medium **We ask you:** Please confirm that emergency changes are peer reviewed and approved by a second engineer before production deployment, and that the two-business-day retrospective review is in addition to that pre-deployment review rather than a substitute for it.
APPSEC-23	APPSEC Is an independent third-party penetration test performed at least annually? When was the most recent test?	Yes. We perform an independent third-party penetration test of the application and AWS environment annually and after major architectural changes. The most recent test was completed in May 2026. Source: information_security_policy.md > 10. Vulnerability management and penetration testing	High

ID	Question	Draft answer	Confidence / what we need
APPSEC-24	APPSEC Do you operate a public bug bounty program?	No. We do not operate a public bug bounty program. We operate a public vulnerability disclosure program at security@brambleway.example and publish a security.txt file. Source: information_security_policy.md > 10. Vulnerability management and penetration testing	Medium **We ask you:** Please confirm that Brambleway does not operate a paid public bug bounty, and that the public vulnerability disclosure program at security@brambleway.example (with security.txt) is the only external researcher reporting channel.
OPS-25	OPS How frequently are vulnerability scans performed, and what are your remediation timelines for critical vulnerabilities?	We scan dependencies and container images automatically on every build and scan infrastructure weekly. Critical vulnerabilities are remediated within 7 days. Source: information_security_policy.md > 10. Vulnerability management and penetration testing	High
OPS-26	OPS Are security logs centrally collected and retained for at least 12 months?	Yes. We centralize AWS CloudTrail, VPC Flow Logs, load balancer logs, and application audit logs in a dedicated logging account and retain them for 13 months. Logs are write-protected with S3 Object Lock. Source: information_security_policy.md > 9. Logging and monitoring	High
IR-27	IR Do you have a documented incident response plan that is tested at least annually?	Yes. We maintain a documented incident response plan covering security and privacy incidents, including defined roles, severity levels, an escalation path, evidence handling, and customer communication. The plan is tested with a tabletop exercise at least annually; the last exercise was in April 2026. It 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

ID	Question	Draft answer	Confidence / what we need
IR-28	IR Within what time frame will you notify customers of a security breach affecting their data?	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. Source: information_security_policy.md > 12. Incident response	High
BCP-29	BCP How often are backups performed and are restores tested?	We run automated daily database snapshots with point-in-time recovery retained for 35 days. We test disaster recovery restores twice a year; the most recent test was in June 2026. Source: information_security_policy.md > 13. Business continuity and disaster recovery	High
BCP-30	BCP What are your RTO and RPO?	Our recovery point objective (RPO) is 1 hour and our recovery time objective (RTO) is 8 hours. Source: information_security_policy.md > 13. Business continuity and disaster recovery	High
VEND-31	VEND Do you assess the security of third-party vendors and subprocessors?	Yes. Our Security Lead reviews vendors and subprocessors. Before onboarding, any vendor that will access Confidential or Customer Data is assessed through a security questionnaire and a review of its SOC 2 or ISO 27001 report, and critical vendors are reassessed annually. Source: information_security_policy.md > 14. Vendor and subprocessor management	High
PRIV-32	PRIV Will you sign a Data Processing Agreement including Standard Contractual Clauses?	*Left blank: not covered by the documents*	Low **We ask you:** Please confirm whether Brambleway will sign a Data Processing Agreement that includes Standard Contractual Clauses, and note any conditions or provide the standard DPA.

ID	Question	Draft answer	Confidence / what we need
PRIV-33	PRIV Do you process protected health information (PHI) or sign Business Associate Agreements?	No. We do not process protected health information under HIPAA. Source: trust_overview.md > Compliance	Medium **We ask you:** Please confirm whether Brambleway signs Business Associate Agreements. Materials state that we do not process protected health information under HIPAA, but they do not address BAAs.
PHYS-34	PHYS Describe the physical security controls at your data centers.	We do not operate our own data centers. All production systems run in AWS data centers, where physical security is AWS's responsibility under the shared responsibility model and is covered by AWS's SOC 2 report. Source: information_security_policy.md > 17. Physical security	High
END-35	END Are company laptops managed with MDM and full-disk encryption?	Yes. We enroll every company laptop in mobile device management (MDM), which enforces full-disk encryption. Source: information_security_policy.md > 16. Endpoints and remote work	High

About the questions. Representative question set written by VendorClerk covering SIG Lite-style topics. It is not the Shared Assessments SIG (a licensed product) and contains no SIG content.
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.