VendorClerk

Brambleway policy pack (fictional)

Fictional. 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.

These three documents are the only evidence the sample drafts were written from. Questions they don't answer (for example cyber insurance, bug bounty, AI training, or SCCs) are flagged in the samples instead of guessed.

Document: information_security_policy.md

Brambleway, Inc. Information Security Policy (FICTIONAL SAMPLE)

> FICTIONAL. Brambleway, Inc. is an invented company created by VendorClerk to demonstrate questionnaire drafting. Nothing in this document describes a real organization, product, person, or audit.

Version 2.0. Owner: VP of Engineering, who also acts as the Security Lead. Approved by the CEO on 2026-03-02. This policy and its supporting procedures are reviewed and re-approved at least once per year, and whenever a significant change to the business, infrastructure, or threat landscape occurs. The policy is published on the internal wiki, acknowledged by every employee and contractor at onboarding, and re-acknowledged annually.

1. Scope and governance

This policy applies to all Brambleway employees, contractors, systems, and all customer data processed by the Brambleway HR onboarding platform. Brambleway has 31 employees and is based in Portland, Oregon (fictional), with a fully remote engineering team in the United States. The VP of Engineering is accountable for the information security and privacy program and reports security metrics and open risks to the CEO and the board quarterly. One full-time security engineer spends 100% of their time on information security; the VP of Engineering spends roughly a third of their time on it. Exceptions to this policy must be requested in writing, risk-assessed, approved by the Security Lead, and given an expiry date of no more than 12 months. The program is aligned with the AICPA SOC 2 Trust Services Criteria and uses the CIS Controls v8 as an implementation guide. Brambleway is not ISO 27001 certified.

2. Policy topics

The information security policy set covers: information classification and handling, acceptable use of information and IT devices, access control, cryptography and key management, secure software development, change management, logging and monitoring, vulnerability management, incident response for both security and privacy incidents, business continuity and disaster recovery, vendor and subprocessor management, human resources security, physical security for the office, data retention and destruction, and compliance with applicable laws and regulations.

3. Risk management

Brambleway performs a formal information security risk assessment at least annually and whenever a major change is introduced (for example a new subprocessor or a new product line). Risks are recorded in a risk register with an owner, likelihood, impact, and treatment decision (mitigate, transfer, accept, or avoid). The risk register is reviewed quarterly by the Security Lead and the CEO. Accepted risks require CEO sign-off.

4. Internal and external assessment

The security engineer performs an internal control assessment every quarter against the SOC 2 control set, covering all systems that store or process customer data. Findings are tracked to closure in the engineering issue tracker. An independent CPA firm performs a SOC 2 Type II examination every year (see the trust overview for the current report period). Brambleway selects auditors through a competitive proposal process and reviews the auditor relationship every three years. Customers under NDA may request the full SOC 2 Type II report; a management summary is available on request.

5. Asset management and data classification

All production infrastructure is defined as code (Terraform) and inventoried automatically from AWS. Company laptops are inventoried in the mobile device management (MDM) system. Data is classified as Public, Internal, Confidential, or Customer Data. Customer Data includes the employee onboarding records customers upload, such as names, contact details, tax forms, and identity documents, and is treated as the most

sensitive class. Adding, changing, or removing production infrastructure requires an approved pull request to the Terraform repository; issuing or retiring a company laptop requires an IT ticket approved by the employee's manager, and the MDM record is updated the same day.

6. Access control

Access is granted on a least-privilege, need-to-know basis according to the person's role. Every access request is ticketed and approved by the employee's manager and the Security Lead. All workforce accounts authenticate through Okta single sign-on, and phishing-resistant multi-factor authentication (WebAuthn security keys) is enforced for every workforce account, including administrators. Production AWS access uses AWS IAM Identity Center with short-lived credentials; there are no long-lived IAM user access keys for humans. Direct production database access is limited to three engineers and requires a just-in-time request that expires after four hours. User access reviews for production systems and critical SaaS tools are performed quarterly; each review revalidates least privilege and checks separation of duties (for example, that no engineer can both approve and deploy their own change). Workforce credentials are managed only through Okta: passwords are never shared, security keys are issued and revoked by IT, and API tokens for automation are stored in AWS Secrets Manager and rotated every 90 days. When someone leaves, the Okta account and all downstream access are disabled within four hours of the termination time, and company laptops are remotely locked; role changes trigger an access review within five business days.

7. Cryptography and key management

Customer data is encrypted 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; this one-year cryptoperiod was chosen in the annual risk assessment, and keys are rotated immediately if compromise is suspected. Encryption uses AWS-managed cryptographic modules validated under FIPS 140-3 and standard TLS libraries maintained by the platform; Brambleway does not implement its own cryptography. Data in transit over public networks is encrypted with TLS 1.2 or higher. Application secrets are stored in AWS Secrets Manager and never committed to source code; secret scanning runs on every pull request.

8. Network and infrastructure security

Production runs in AWS us-west-2 (Oregon) with a warm standby in us-east-1. Production, staging, and development are separate AWS accounts under AWS Organizations. Databases and application servers sit in private subnets with no public IP addresses; inbound traffic reaches the application only through an AWS Application Load Balancer protected by AWS WAF. Security groups deny by default. Infrastructure changes are made only through Terraform via the CI pipeline.

9. Logging and monitoring

AWS CloudTrail, VPC Flow Logs, load balancer logs, and application audit logs are centralized in a dedicated logging account and retained for 13 months. Logs are write-protected with S3 Object Lock. Amazon GuardDuty and AWS Security Hub are enabled in all accounts and correlate CloudTrail, VPC Flow Log, and DNS events to detect anomalous activity; application audit logs feed alert rules for unusual sign-in patterns and bulk data exports, and alerts route to the on-call engineer through PagerDuty 24×7. Endpoint detection and response (EDR) runs on all company laptops.

10. Vulnerability management and penetration testing

Dependencies and container images are scanned automatically on every build, and infrastructure is scanned weekly. Remediation targets: critical within 7 days, high within 30 days, medium within 90 days. An independent third-party penetration test of the application and AWS environment is performed annually and after major architectural changes; the most recent test was completed in May 2026, and all high and critical findings were remediated and retested. Brambleway runs a public vulnerability disclosure program at security@brambleway.example and publishes a security.txt file.

11. Change management and secure development

The change management process is documented in the engineering handbook and classifies changes as standard, normal, or emergency according to impact. All code changes go through pull requests that require review and approval by a second engineer who did not write the change, and passing automated tests, static analysis (SAST), and dependency scanning before merge. Changes that touch authentication, authorization, cryptography, or customer data handling also require approval from the security engineer, who sits on the weekly change review. Deployments are automated through the CI/CD pipeline; engineers cannot deploy from their laptops. Emergency changes are reviewed retrospectively within two business days. Pull request history, approvals, and deployment records are retained for at least three years. Developers complete secure coding training (OWASP Top 10) annually. The secure development lifecycle documented in the engineering handbook covers every phase: security requirements and threat modeling during design for features that touch customer data, secure coding standards, code review, automated security testing, controlled deployment, and post-release monitoring. Privacy by design is part of the design review: new features collect only the personal data needed and default to the most restrictive sharing setting.

12. Incident response

Brambleway maintains 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 tested with a tabletop exercise at least annually; the last exercise was in April 2026. Brambleway has an incident response retainer with an external forensics firm for investigations that exceed internal capacity. The incident response plan is approved by the CEO, reviewed annually, and communicated to every engineer during on-call onboarding. Brambleway does not have a separate e-discovery procedure; legal holds are handled case by case with outside counsel. Affected customers are notified without undue delay and in any case within 72 hours of confirming a security incident that affects their data, as committed in the Data Processing Addendum.

13. Business continuity and disaster recovery

Amazon RDS runs Multi-AZ with automated daily snapshots and point-in-time recovery for 35 days. Backups are encrypted and copied to us-east-1. Recovery objectives: RPO 1 hour, RTO 8 hours. A disaster recovery restore test is performed twice a year; the last test was in June 2026. Business-critical infrastructure is redundant within the primary region (multiple AWS Availability Zones) and geographically dispersed through the warm standby environment in us-east-1, roughly 2,000 miles from us-west-2, following AWS's well-architected reliability guidance.

14. Vendor and subprocessor management

The Security Lead is responsible for reviewing 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. Written contracts with all subprocessors require them to protect the confidentiality, integrity, and security of the data they process, to notify Brambleway of incidents, and to follow data protection terms at least as protective as Brambleway's own Data Processing Addendum.

15. Human resources security

Every role with access to Confidential or Customer Data has a written job description that defines its security responsibilities. 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; other contractors do not. All employees and contractors sign confidentiality agreements and complete security and privacy awareness training at onboarding and annually, plus quarterly phishing simulations. The awareness program is owned by the security engineer, approved by the VP of Engineering, updated each year with current threats, and evaluated through completion tracking and phishing-simulation results reported to the CEO. Interns and temporary staff complete the same training before receiving access. Violations of security policy are handled through a documented disciplinary process that can lead to termination.

16. Endpoints and remote work

The Endpoint and Remote Work Standard, part of this policy set, applies to every company laptop, and it is approved and reviewed on the same annual cycle. All laptops are enrolled in MDM, which enforces full-disk encryption, automatic OS updates, screen lock after five minutes, and EDR. Personal devices may access only email and chat through Okta with device checks and may never store Customer Data. Remote employees must work from private networks or use the company VPN on public Wi-Fi, and may not print Customer Data.

17. Physical security

Brambleway does not operate its own data centers; all production systems run in AWS data centers, and physical security for them is AWS's responsibility under the shared responsibility model and is covered by AWS's SOC 2 report. The small Portland office uses badge access and stores no customer data.

18. Data retention, deletion, and privacy

Customer Data is retained for the life of the customer's subscription. Customers can delete individual records at any time; deleted records are purged from production within 30 days and from backups within 35 days. On contract termination, Customer Data is deleted within 30 days unless the customer requests an export first. Brambleway never handles physical storage media for production data: AWS sanitizes and destroys decommissioned media under its own procedures (aligned with NIST 800-88), and deleted data is additionally protected by destruction of the associated encryption keys when a customer's dedicated KMS key is retired. Retired company laptops are wiped with the MDM's cryptographic erase before reuse or recycling. Brambleway publishes a privacy notice at brambleway.example/privacy and a Data Processing Addendum. Brambleway acts as a processor of the personal data its customers upload.

Document: application_security.md

Brambleway HR Application Security Overview (FICTIONAL SAMPLE)

> FICTIONAL. Brambleway, Inc. is an invented company created by VendorClerk to demonstrate questionnaire drafting.

Architecture and frameworks

Brambleway HR is a Ruby on Rails 8 application with a React front end, served over HTTPS only. It stores data in PostgreSQL (Amazon RDS) and uploaded documents in Amazon S3.

TLS configuration

TLS terminates at the AWS Application Load Balancer, which uses the ELBSecurityPolicy-TLS13-1-2-2021-06 policy: only TLS 1.2 and TLS 1.3 with forward-secret (ECDHE) cipher suites. Certificates and private keys are managed by AWS Certificate Manager, so private keys are never stored on web servers. Traffic between the load balancer and application containers is re-encrypted with TLS inside the VPC. HSTS is enabled

with a one-year max-age, and the application serves no mixed content. The TLS configuration is reviewed every quarter with an external scanner.

Authentication

Customer administrators can require SAML 2.0 single sign-on (Okta, Microsoft Entra ID, Google Workspace) or Sign in with Google (OpenID Connect via the omniauth library) for their organization. Username and password login is also available. Passwords must be at least 12 characters and are checked against a breached-password list; there are no composition rules. Users can change their password from account settings. Passwords are hashed with bcrypt (cost 12). New users receive a one-time, expiring invitation link and set their own password; Brambleway never sends initial passwords. Password recovery uses a single-use reset link emailed to the verified address that expires after 30 minutes. Users can enroll TOTP or WebAuthn MFA, and customer administrators can make MFA mandatory.

Sessions

Session IDs are generated by the Rails framework using a cryptographically secure random number generator (SecureRandom). Session cookies are set with the Secure, HttpOnly, and SameSite=Lax attributes. Sessions time out after 30 minutes of inactivity and after 12 hours absolute. Logging out invalidates the session on the server, not just in the browser.

Authorization

Every request is authorized server-side. Tenant isolation (horizontal access control) is enforced by scoping all queries to the authenticated customer account in a central authorization layer (Pundit policies), and automated tests verify that users cannot read or modify another tenant's records. Role-based permissions (vertical access control) separate administrators, HR managers, and new hires, and are enforced on the server for every action.

Common web vulnerabilities

All state-changing requests are protected against cross-site request forgery with Rails' synchronizer token pattern plus SameSite cookies. Cross-site scripting is prevented through automatic output escaping in Rails views and React, and a strict Content Security Policy. Every response sets an explicit Content-Type and UTF-8 character set. JSON responses are never served as JavaScript. The application sends X-Frame-Options: DENY and a frame-ancestors 'none' CSP directive to prevent clickjacking. SQL injection is prevented by using the ActiveRecord ORM with parameterized queries; raw SQL string concatenation is blocked by a static analysis rule (Brakeman) in CI. No browser plugins are required.

File uploads

Users upload onboarding documents (PDF, JPG, PNG, and HEIC only, maximum 20 MB). Files are stored in a private S3 bucket, never on the web servers, and are served to authorized users only through short-lived pre-signed URLs from a separate domain. File types are enforced by checking the file's content signature (magic bytes), not just the extension, and every upload is scanned for malware.

Testing

The codebase has automated unit and integration tests with about 85% line coverage, including security-specific tests for authorization, tenant isolation, CSRF, and output escaping. Engineers and QA review security impact during release testing and complete annual OWASP Top 10 training. After launch, the application is monitored with error tracking, anomaly alerts on authentication failures, and AWS WAF metrics.

Document: trust_overview.md

Brambleway Trust Overview (FICTIONAL SAMPLE)

> FICTIONAL. Brambleway, Inc. is an invented company created by VendorClerk to demonstrate questionnaire drafting. No real company, audit, or report is described here.

Product

Brambleway HR is a multi-tenant SaaS web application that small and mid-sized businesses use to onboard new employees: offer letters, tax and identity forms, e-signatures, and onboarding checklists. It is used by about 1,200 customer companies. Customers are the data controllers; Brambleway is the processor.

Compliance

Brambleway has completed a SOC 2 Type II examination covering the Security, Availability, and Confidentiality Trust Services Criteria for the period 2025-07-01 to 2026-06-30, performed by an independent CPA firm (fictional: Hartwell & Ames LLP). The report contained no exceptions. Brambleway is not ISO 27001 certified, is not PCI DSS in scope (card payments are handled entirely by Stripe), and does not process protected health information under HIPAA.

Hosting and data location

All customer data is stored and processed in the United States, in AWS us-west-2 with backups and a warm standby in us-east-1.

Subprocessors

AWS (hosting), Stripe (billing, no customer HR data), SendGrid (transactional email), Okta (workforce identity only), and Zendesk (support tickets). The current list is published at brambleway.example/subprocessors, and customers receive 30 days' notice of new subprocessors.

Security contacts

Security issues and vulnerability reports: security@brambleway.example. Brambleway acknowledges vulnerability reports within two business days and does not pursue legal action against good-faith researchers.

Availability

The platform's availability target is 99.9% per month, published on a public status page.

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