Information Security Policy & Procedures

Identifying, Mitigating, and Monitoring Information Security Risks

Version: 1.0

Effective Date: March 10, 2026

Last Reviewed: March 10, 2026

Next Review: March 2027

Classification: Public

SRVAUDIT LLC

Table of Contents

01 Purpose & Scope

1.1 Purpose

This Information Security Policy establishes the framework for protecting the confidentiality, integrity, and availability of information assets owned, operated, and managed by **srvAudit LLC** and all of its doing-business-as (DBA) entities, including but not limited to:

- **DNSApe** — DNS diagnostics and network tools platform
- **EC2Info** — AWS EC2 instance reference and pricing data
- **MemorialNow** — Online memorial and obituary platform
- **Apache Drones** — Commercial drone services
- **MoneyFly** — Personal finance and wealth building platform
- **Sovid** — Video processing and social video platform

This policy defines the security controls, procedures, and responsibilities required to identify, mitigate, and continuously monitor information security risks relevant to our business operations, client data, and technology infrastructure.

1.2 Scope

This policy applies to:

- All information systems, networks, applications, and data under srvAudit LLC's operational control
- All employees, contractors, subcontractors, and third-party personnel who access company systems or data
- All environments including production, staging, development, and disaster recovery
- Cloud infrastructure (AWS), serverless compute (Lambda via Laravel Vapor), databases, storage, DNS, and email services
- Client data processed through proposals, contracts, payments, and service delivery

1.3 Regulatory & Contractual Context

srvAudit LLC aligns its security practices with applicable regulatory requirements and industry standards, including:

- **PCI DSS** — Payment card data handled via Stripe (PCI-compliant processor); srvAudit does not store, process, or transmit cardholder data directly
- **Arizona Data Breach Notification Law** (A.R.S. § 18-552) — Notification obligations for personal information breaches
- **CAN-SPAM Act** — Commercial email compliance
- **NIST Cybersecurity Framework (CSF)** — Reference framework for risk management

02 Information Security Organization

2.1 Information Security Officer (ISO)

The owner/principal of srvAudit LLC serves as the ISO with overall accountability for:

- Establishing and maintaining this policy and supporting procedures
- Conducting risk assessments and authorizing risk treatment plans
- Ensuring compliance with applicable laws and contractual obligations
- Reviewing and approving access to production systems
- Leading incident response and breach notification activities

2.2 System Administrators / Developers

Personnel with privileged access are responsible for:

- Implementing security controls as defined in this policy
- Reporting security incidents or vulnerabilities immediately
- Following secure development practices
- Maintaining up-to-date systems and dependencies

2.3 Contractors & Third Parties

External personnel must:

- Agree to confidentiality and acceptable use terms before accessing systems
- Operate within the principle of least privilege
- Return or destroy all company data upon engagement termination

03 Risk Management

3.1 Risk Identification

srvAudit LLC maintains an ongoing risk identification process that includes:

- **Asset inventory** — Maintaining a catalog of information assets including servers, databases, applications, code repositories, and third-party services
- **Threat assessment** — Identifying potential threats (unauthorized access, data loss, service disruption, malware, social engineering, insider threats)
- **Vulnerability scanning** — Regular automated scanning of infrastructure and dependencies (Composer audit, npm audit, AWS Inspector)
- **Change-driven review** — Evaluating security implications when introducing new services, integrations, or infrastructure changes

3.2 Risk Assessment & Scoring

Identified risks are assessed using a qualitative risk matrix based on **likelihood** (rare, unlikely, possible, likely, almost certain) and **impact** (negligible, minor, moderate, major, critical). Risks scoring "high" or "critical" require documented treatment plans with assigned owners and deadlines.

3.3 Risk Treatment

For each identified risk, one of the following treatment strategies is applied:

- **Mitigate** — Implement controls to reduce likelihood or impact to acceptable levels
- **Transfer** — Shift risk to a third party (e.g., cyber liability insurance, PCI-compliant payment processor)
- **Accept** — Formally acknowledge and document residual risk when cost of mitigation exceeds potential impact
- **Avoid** — Eliminate the risk by discontinuing the activity or removing the asset

3.4 Risk Monitoring

Risk posture is continuously monitored through:

- **Automated alerts** — AWS CloudWatch, GuardDuty, and application-level error monitoring
- **Dependency audits** — Automated Composer and npm vulnerability scanning in CI/CD pipelines
- **Periodic review** — Formal risk register review at least quarterly, or upon significant changes
- **Log analysis** — Review of access logs, authentication events, and anomalous activity

04 Access Control

4.1 Principles

- **Least privilege** — Users and systems receive only the minimum access required to perform their function
- **Zero trust** — No implicit trust is granted based on network location; every request is verified regardless of origin
- **Separation of duties** — Critical operations require multiple parties or approval steps where feasible
- **Need-to-know** — Access to sensitive data is restricted to personnel with a demonstrated business need

4.2 Authentication

- All production systems require strong authentication (minimum 12-character passwords or SSH key-based authentication)
- Multi-factor authentication (MFA) is required for AWS root and IAM accounts, Vapor dashboard, Stripe, domain registrars, and all critical SaaS services
- Application-level MFA (TOTP) is available for all user accounts via Laravel Fortify two-factor authentication
- API access uses scoped OAuth tokens (Laravel Sanctum / Passport) with appropriate expiration
- Non-human authentication via OAuth tokens, IAM roles, and TLS-encrypted service-to-service communication

4.3 Authorization

- Role-based access control (RBAC) is implemented across all applications with defined user roles and permission sets
- Centralized identity management: AWS IAM for infrastructure access, Laravel Fortify for application-level authentication
- AWS IAM policies follow least-privilege principles with service-specific roles
- Database access is restricted to application service accounts; direct database access is prohibited in production except for emergency maintenance

4.4 Access Reviews

- User access rights are reviewed quarterly

- Systematic de-provisioning upon role change or termination — access revoked within 24 hours, shared credentials rotated immediately
- AWS IAM access keys and credentials are rotated at least every 90 days
- Unused accounts are disabled after 90 days of inactivity

4.5 Zero Trust Architecture

srvAudit LLC implements zero trust principles across its infrastructure:

- Serverless architecture (AWS Lambda) provides ephemeral, isolated execution environments with no persistent network access or standing credentials
- All service-to-service communication is authenticated and encrypted — no implicit trust based on network location
- AWS IAM roles enforce identity-based access policies; no shared or ambient credentials
- Application requests are authenticated and authorized individually regardless of source network
- Infrastructure access requires explicit identity verification (MFA + SSH keys) even from trusted networks

05 Data Protection

5.1 Data Classification

- **Confidential** — Client personal information, payment data (handled by Stripe), contracts, credentials, API keys, encryption keys
- **Internal** — Business proposals, pricing, internal communications, source code, infrastructure configuration
- **Public** — Marketing content, published documentation, public-facing application interfaces

5.2 Encryption

- **In transit** — All web traffic is encrypted via TLS 1.2+ (enforced via HTTPS). Internal service communication uses encrypted channels.
- **At rest** — AWS RDS databases use AES-256 encryption. S3 buckets use server-side encryption (SSE-S3 or SSE-KMS). EBS volumes are encrypted.
- **Application-level** — Sensitive fields (e.g., API tokens, webhook secrets) are encrypted using Laravel's built-in encryption (AES-256-CBC via APP_KEY)

5.3 Data Retention & Disposal

- Client data is retained only for the duration required by the business relationship and applicable legal obligations
- Upon contract termination, client data is securely deleted within 90 days unless a legal hold applies
- Backups follow a 30-day retention cycle; expired backups are automatically purged
- Development and staging environments do not contain production client data; anonymized or synthetic data is used for testing

5.4 Payment Data

> srvAudit LLC does not directly store, process, or transmit credit card numbers. All payment processing is delegated to **Stripe**, a PCI DSS Level 1 certified service provider. Payment forms use Stripe Elements / Payment Intents, which tokenize card data client-side before it reaches our servers. We store only Stripe customer IDs, payment intent IDs, and transaction metadata.

06 Infrastructure Security

6.1 Cloud Architecture

Production applications are deployed on **AWS** using **Laravel Vapor** (serverless via AWS Lambda), providing inherent security benefits including automatic patching, ephemeral execution environments, and AWS-managed infrastructure hardening.

6.2 Network Security

- AWS Security Groups enforce strict ingress/egress rules (default deny, explicit allow)
- EC2 instances (where used) are hardened: SSH key-only authentication, non-default ports where appropriate, automatic security updates
- CloudFront CDN provides DDoS mitigation (AWS Shield Standard) and edge-level TLS termination
- VPC configurations isolate production resources from public internet where direct access is not required

6.3 Patch Management

- Lambda-based (Vapor) deployments inherit AWS-managed runtime patching
- EC2 instances receive security patches via automated update mechanisms (unattended-upgrades on Ubuntu)
- Application dependencies are monitored for known vulnerabilities and updated promptly (Composer audit, npm audit)
- Critical security patches are applied within 48 hours of disclosure; high-severity within 7 days

6.4 Logging & Monitoring

- Application logs are captured via Laravel's logging subsystem
- AWS CloudTrail records all API activity across AWS accounts
- CloudWatch monitors infrastructure metrics with alerting thresholds for anomalous patterns
- Access logs (HTTP, SSH, database) are retained for a minimum of 90 days

07 Application Security

7.1 Secure Development Lifecycle

- **Input validation** — All user input is validated and sanitized using Laravel's validation framework
- **Output encoding** — Blade templating engine auto-escapes output to prevent XSS
- **SQL injection prevention** — Eloquent ORM and parameterized queries are used exclusively; raw SQL is prohibited without review
- **CSRF protection** — All state-changing requests are protected by Laravel's CSRF middleware
- **Mass assignment protection** — Models use explicit `$fillable` attributes

7.2 Dependency Management

- Third-party packages are sourced from trusted registries (Packagist, npm)
- `composer audit` and `npm audit` are run before each production deployment
- Lock files (`composer.lock`, `package-lock.json`) are committed to ensure reproducible builds

7.3 Secrets Management

- Application secrets and API keys are stored in environment variables, never in source code
- Production environment variables are managed through Laravel Vapor's encrypted environment system or AWS SSM Parameter Store (SecureString)
- Secrets are rotated on a regular schedule and immediately upon suspected compromise

08 Incident Response

8.1 Incident Classification

- **Critical** — Confirmed data breach, active exploitation, ransomware, unauthorized access to production data
- **High** — Suspected breach, vulnerability actively being exploited in the wild, compromised credentials
- **Medium** — Detected vulnerability requiring patching, suspicious activity under investigation
- **Low** — Policy violation, failed attack attempt, informational security event

8.2 Response Procedures

1. **Detection & Triage** — Identify the incident, assess severity, and assign an incident lead
2. **Containment** — Isolate affected systems to prevent further damage (revoke access, disable compromised accounts, block malicious IPs)
3. **Eradication** — Remove the root cause (patch vulnerability, remove malware, rotate credentials)
4. **Recovery** — Restore systems from verified clean backups; validate integrity before returning to production
5. **Post-Incident Review** — Document lessons learned, update controls, and revise risk register within 14 days

8.3 Breach Notification

> In the event of a confirmed breach involving personal information, srvAudit LLC will comply with the **Arizona Data Breach Notification Law (A.R.S. § 18-552)**, which requires notification to affected individuals within 45 days of breach discovery. If the breach affects more than 1,000 individuals, the Arizona Attorney General will also be notified. Affected clients will be notified directly via email with details of the breach, data involved, and recommended protective actions.

8.4 Communication

- All incident communications are coordinated through the ISO
- External communications (client notifications, regulatory filings) require ISO approval
- Incident details are shared internally on a need-to-know basis only

09 Business Continuity & Disaster Recovery

9.1 Backups

- Production databases (RDS) are backed up daily via automated snapshots with 30-day retention
- S3 data is protected by bucket versioning and cross-region replication where business-critical
- Backup restoration is tested at least semi-annually

9.2 Availability

- Serverless architecture (Lambda/Vapor) provides automatic scaling and high availability across multiple availability zones
- CloudFront CDN ensures global edge availability and mitigates regional outages for static assets
- RDS Multi-AZ deployments provide database failover capability

9.3 Recovery Objectives

- **Recovery Time Objective (RTO)** — 4 hours for critical systems
- **Recovery Point Objective (RPO)** — 24 hours (daily backup frequency)

10 Third-Party & Vendor Management

10.1 Vendor Assessment

Third-party services that process, store, or transmit company or client data are evaluated for security posture before engagement. Key vendors include:

VENDOR	ROLE	CERTIFICATION
AWS	Cloud infrastructure	SOC 2 Type II, ISO 27001, PCI DSS L1
Stripe	Payment processing	PCI DSS Level 1
Laravel Vapor	Serverless deployment	Operates in customer AWS account
Cloudflare	DNS & CDN	SOC 2 Type II
OneSignal	Push notifications	No sensitive data transmitted

10.2 Ongoing Monitoring

- Critical vendor security certifications are verified annually
- Vendor access is reviewed as part of quarterly access reviews
- Vendor security incidents are monitored via public advisories and direct communication

11 Personnel Security

11.1 Onboarding

- All personnel with system access must acknowledge this Information Security Policy before receiving credentials
- Access is provisioned based on role with least-privilege defaults
- Contractors sign confidentiality / NDA agreements covering data handling obligations

11.2 Security Awareness

- Personnel are briefed on phishing, social engineering, and secure credential handling
- Security best practices are documented and accessible to all team members
- Significant security events or emerging threats are communicated promptly

11.3 Offboarding

- Access is revoked within 24 hours of engagement termination
- All company-owned equipment and data are returned or confirmed destroyed
- Shared credentials are rotated immediately upon departure of any privileged user

12 Compliance & Audit

12.1 Internal Audits

- Security controls are audited internally at least annually
- Audit scope includes access controls, encryption implementation, logging, backup integrity, and incident response readiness
- Findings are documented with remediation timelines and tracked to closure

12.2 External Assessments

- Third-party penetration testing or vulnerability assessments are conducted as required by client contracts or risk profile
- Results are reviewed by the ISO and remediated per the risk treatment framework

12.3 Recordkeeping

- Security policies, risk assessments, incident reports, and audit findings are retained for a minimum of 3 years
- Records are stored securely and accessible only to authorized personnel

13 Policy Governance

13.1 Review Cycle

This policy is reviewed and updated **at least annually**, or upon:

- Significant changes to business operations, technology stack, or threat landscape
- A security incident that reveals policy gaps
- Changes in applicable laws or regulatory requirements

- Client or contractual requirements

13.2 Approval

This policy is approved and authorized by the principal of srvAudit LLC in their capacity as Information Security Officer.

13.3 Version History

VERSION	DATE	DESCRIPTION
1.0	March 10, 2026	Initial policy creation and publication

> **Questions or Security Concerns**
> For questions about this policy, to report a security concern, or to request a copy of our risk register, contact us at **security@srvaudit.com**.