

Security Whitepaper

Enterprise-Grade Data Protection & Compliance

Version 1.0 | February 2026

Document Information

Document Type:	Security Whitepaper
Classification:	Public
Prepared By:	ObituaryMonitor Security Team
Contact:	security@obituarymonitor.com

Executive Summary

ObituaryMonitor provides enterprise-grade obituary monitoring services for legal professionals, insurance companies, and individuals. This document outlines our comprehensive security framework and data protection measures.

Our security architecture is built on industry best practices, utilizing AES-256 encryption at rest and TLS 1.3 for data in transit. We partner with infrastructure providers who maintain SOC 2 Type II certifications (Netlify, Neon, Postmark) and PCI DSS Level 1 certification (Stripe). Note: ObituaryMonitor itself has not undergone a SOC 2 audit.

Table of Contents

- 1. Security Architecture Overview - - - - -3
- 2. Data Encryption Standards - - - - -4
- 3. Infrastructure Security - - - - -5
- 4. Access Control & Authentication - - - - -6
- 5. Data Privacy & Compliance - - - - -7
- 6. Incident Response - - - - -8
- 7. Vendor Security - - - - -9
- 8. Infrastructure Partner Security - - - - -10
- 9. Data Retention & Deletion - - - - -11
- 10. Contact Information - - - - -12

1. Security Architecture Overview

ObituaryMonitor's security architecture follows a defense-in-depth approach, implementing multiple layers of security controls to protect data at every level of our technology stack.

Key Security Principles:

- Least Privilege Access: All system components operate with minimal required permissions
- Defense in Depth: Multiple overlapping security controls at each layer
- Secure by Default: Security is built into the design, not added as an afterthought
- Zero Trust Architecture: All access requests are verified regardless of source
- Continuous Monitoring: Real-time threat detection and response capabilities

Our architecture is designed to meet the security requirements of enterprise customers including law firms, insurance companies, and financial institutions handling sensitive client data.



2. Data Encryption Standards

Encryption in Transit

All data transmitted between clients and our servers is encrypted using TLS 1.3, the latest and most secure transport layer security protocol. We enforce HTTPS for all connections and implement HSTS (HTTP Strict Transport Security) headers.

- Protocol: TLS 1.3 (TLS 1.2 minimum for legacy compatibility)
- Cipher Suites: ECDHE key exchange with AES-256-GCM
- Certificate: 2048-bit RSA with SHA-256 signature
- Perfect Forward Secrecy: Enabled for all connections

Encryption at Rest

All stored data is encrypted using AES-256 encryption, the same standard used by financial institutions and government agencies worldwide.

- Algorithm: AES-256-GCM
- Key Management: Hardware Security Modules (HSM) managed by cloud provider
- Key Rotation: Automatic key rotation every 90 days
- Backup Encryption: All backups encrypted with separate encryption keys

Password Security

- Hashing Algorithm: bcrypt with high work factor (cost factor 12+)
- Salt: Unique per-password random salt
- Storage: Only hashed passwords stored; plaintext never logged or stored

3. Infrastructure Security

Our infrastructure is built on industry-leading cloud platforms with robust security measures and certifications.

Cloud Infrastructure Partners:

Netlify (Application Hosting)

- SOC 2 Type II certified
- Automatic DDoS protection
- Edge network with global distribution
- Automatic HTTPS/TLS certificate management

Neon (Database)

- SOC 2 Type II certified PostgreSQL
- Encryption at rest (AES-256)
- Point-in-time recovery
- Automatic failover and high availability

Stripe (Payment Processing)

- PCI DSS Level 1 certified
- Tokenization of sensitive card data
- No card data touches our servers

Network Security:

- Web Application Firewall (WAF) protection
- Rate limiting and throttling
- IP reputation filtering
- Automated threat detection

4. Access Control & Authentication

Role-Based Access Control (RBAC)

ObituaryMonitor implements granular role-based access control for all user accounts:

- Owner: Full administrative access, billing management
- Admin: User management, settings configuration
- Member: Standard access to watches and matches
- Viewer: Read-only access to reports and data

Session Management:

- Secure, HTTP-only session cookies
- Automatic session timeout after 30 minutes of inactivity
- Concurrent session limits (configurable per organization)
- Session invalidation on password change

API Authentication:

- Unique API keys per integration
- Revocable at any time from dashboard
- Scoped permissions per key
- Request signing for webhook verification

Audit Logging:

- All authentication events logged
- Login attempts (successful and failed)
- Permission changes tracked
- Data access and modifications recorded
- 90-day retention for security logs

5. Data Privacy & Compliance

Privacy Principles:

- No Data Selling: We never sell personal information to third parties
- Minimal Collection: We only collect data necessary to provide our service
- Purpose Limitation: Data is only used for stated purposes
- Transparency: Clear privacy policy available at obituarymonitor.com/privacy

CCPA Compliance (California Consumer Privacy Act):

- Right to Know: Users can request information about data collection
- Right to Delete: Users can request deletion of their personal data
- Right to Opt-Out: Users can opt-out of any data sharing
- Non-Discrimination: No service degradation for exercising privacy rights

GDPR Readiness (General Data Protection Regulation):

- Lawful Basis: Processing based on contract performance or legitimate interest
- Data Subject Rights: Access, rectification, erasure, portability
- Data Protection Officer: Available for EU/UK inquiries
- Standard Contractual Clauses: Available for international transfers

Data Processing Agreements (DPA):

Custom DPAs available for enterprise customers upon request.

Healthcare:

We don't currently process protected health information, and we do not offer Business Associate Agreements. Contact us to discuss healthcare use cases.

6. Incident Response

Incident Response Plan:

ObituaryMonitor maintains a documented incident response plan that includes:

1. Detection & Analysis
 - Automated monitoring and alerting systems
 - Real-time threat detection
 - Log analysis and anomaly detection
2. Containment
 - Immediate isolation of affected systems
 - Preservation of forensic evidence
 - Prevention of further damage
3. Eradication & Recovery
 - Root cause analysis
 - System restoration from clean backups
 - Verification of system integrity
4. Post-Incident Activities
 - Lessons learned documentation
 - Process improvement implementation
 - Stakeholder communication

Breach Notification:

In the event of a data breach, we will:

- Notify affected users within 72 hours as required by applicable laws
- Provide details about the nature of the breach
- Explain steps being taken to remediate
- Offer guidance on protective measures users can take

Security Incident Reporting:

Report security concerns to: security@obituarymonitor.com

7. Vendor Security

Third-Party Vendor Assessment:

All vendors with access to customer data undergo security review including:

- Security certification verification (SOC 2, ISO 27001, etc.)
- Data handling practices review
- Contractual security requirements
- Regular reassessment (annual minimum)

Current Vendor Certifications:

Vendor	Service	Certification
Netlify	Hosting	SOC 2 Type II
Neon	Database	SOC 2 Type II
Stripe	Payments	PCI DSS Level 1
Postmark	Email	SOC 2 Type II

Subprocessor List:

A complete list of subprocessors is available upon request for enterprise customers.

Vendor Security Requirements:

All vendors must:

- Maintain current security certifications
- Implement encryption for data at rest and in transit
- Provide timely notification of security incidents
- Support our data deletion requirements

8. Infrastructure Partner Security

Note: ObituaryMonitor has not undergone a SOC 2 audit. The certifications listed below are held by our infrastructure and payment partners.

Infrastructure Partner Certifications:

Our infrastructure is built on platforms that maintain industry certifications:

- Netlify (Hosting): SOC 2 Type II certified
- Neon (Database): SOC 2 Type II certified
- Stripe (Payments): PCI DSS Level 1 certified
- Postmark (Email): SOC 2 Type II certified

Payment Security:

We use Stripe for all payment processing. Stripe is PCI DSS Level 1 certified, the highest level of certification in the payment card industry. Credit card data never touches our servers.

Our Security Practices:

While we have not completed a SOC 2 audit, we implement security controls aligned with industry frameworks:

- Encryption at rest (AES-256) and in transit (TLS 1.3)
- Role-based access control (RBAC)
- Comprehensive audit logging
- Regular security reviews

Security Questionnaires:

We can complete custom security questionnaires upon request.

Contact security@obituarymonitor.com for documentation.

9. Data Retention & Deletion

Data Retention Periods:

Data Type	Retention Period
Account Data	Active account + 30 days
Watch List Data	Active watch + 1 year archived
Match History	Subscription duration + 2 years
Audit Logs	7 years (legal compliance)
Payment Records	7 years (financial regulations)
Security Logs	90 days

Data Deletion:

Upon account deletion request:

- Account data deleted within 30 days
- Archived data purged according to retention schedule
- Anonymized analytics data may be retained
- Legal hold exceptions apply where required by law

Right to Erasure:

Users can request data deletion by:

- Using the account deletion feature in Settings
- Contacting support@obituarymonitor.com
- Contacting privacy@obituarymonitor.com for GDPR requests

Data Portability:

Users can export their data in JSON or CSV format from the dashboard.

10. Contact Information

Security Team

For security concerns, vulnerability reports, or security questionnaires:

Email: security@obituarymonitor.com

Response Time: Within 24 hours for security matters

Privacy Team

For privacy-related inquiries, GDPR/CCPA requests, or DPA negotiations:

Email: privacy@obituarymonitor.com

Data Protection Officer: dpo@obituarymonitor.com

General Support

For general questions or technical support:

Email: support@obituarymonitor.com

Help Center: <https://obituarymonitor.com/help>

Enterprise Sales

For enterprise security documentation, custom agreements, or compliance inquiries:

Email: sales@obituarymonitor.com

Website: <https://obituarymonitor.com/pricing>

Responsible Disclosure:

If you discover a security vulnerability, please report it responsibly to security@obituarymonitor.com. We appreciate security researchers who help us keep our platform secure.

This document is provided for informational purposes. ObituaryMonitor reserves the right to update security practices at any time. For the most current information, please contact our security team or visit obituarymonitor.com/security.