KMS Lighthouse®

KMS Lighthouse Security Policy

Last updated: June 2026

Security is fundamental to how KMS Lighthouse builds and operates its knowledge management platform. We maintain an information security program built on recognized industry standards, validated by independent third-party audits and penetration testing. This page summarizes the controls and assurances that protect customer data across the KMS Lighthouse service.

SOC 2 Type 2 **ISO/IEC 27001:2022** **Independent Penetration Testing**

GDPR and CCPA aligned

Certifications and independent assurance

- **SOC 2 Type 2.** KMS Lighthouse Ltd. maintains a SOC 2 Type 2 attestation covering the Security trust services category for its knowledge management system. The examination is performed by an independent auditor (a member firm of PricewaterhouseCoopers), and coverage is kept current through a bridge letter between examination periods.
- **ISO/IEC 27001:2022.** KMS Lighthouse operates under the Aman Group Information Security Management System (ISMS), which is certified to ISO/IEC 27001:2022 by an accredited certification body (SII-QCD, accredited under ANAB and IAF/IQNET). The certified ISMS covers software development and IT services.
- **Independent penetration testing.** The KMS Lighthouse web application and REST API undergo regular manual penetration testing by independent security firms, conducted in line with the OWASP testing methodology. Findings are remediated and re-tested until resolved, and internal network assessments are validated to confirm that critical and high-risk findings are addressed.

> The SOC 2 Type 2 report, ISO/IEC 27001 certificate, and penetration test summaries are available to current and prospective customers on request under a non-disclosure agreement.

Organizational security

- A formal information security risk management process governs how risks are identified, ranked, and treated.
- Security policies are reviewed regularly and communicated to all personnel.
- Employee access follows least-privilege principles, with formal provisioning, modification, and de-provisioning processes.
- Multi-factor authentication protects access to code repositories, infrastructure, and credential management.

Access control and authentication

- Access to production systems and customer data is restricted to authorized personnel on a need-to-know basis.
- Authentication mechanisms enforce account-lockout and password-complexity controls.
- Administrative access is segregated, logged, and reviewed.

Data protection and encryption

- Customer data is encrypted in transit using TLS.
- Data at rest is encrypted using industry-standard disk encryption.
- The platform is designed to minimize the personal data it processes and to avoid storing unnecessary identifiers.

Secure development

- Secure coding practices account for common vulnerability classes, including the OWASP Top 10.
- All production code changes are peer-reviewed by an additional reviewer before deployment.
- A formal change-management process governs review and approval of changes before they reach production.
- Patch management is governed by a defined SLA policy, and patching activities are carried out accordingly.

Infrastructure and hosting

- The KMS Lighthouse service is hosted on enterprise-grade cloud infrastructure operated by leading providers.
- Network boundaries are protected by firewalls, and unsupported operating systems and software are not used in the production environment.
- Annual penetration testing is performed against the application and its supporting infrastructure.

Monitoring and incident response

- Event logging is enabled across system components supporting the service.
- Logs are reviewed on a regular cadence by automated tooling and personnel to detect potential security events.
- Detected security events trigger automated alerts for triage.
- A formal, documented security incident response process is established and maintained.
- Data breaches are reported to relevant authorities and affected parties in line with applicable regulatory requirements.

Business continuity and disaster recovery

- A documented disaster recovery plan, including a backup and restore strategy, supports the availability of the service.

Privacy and regulatory compliance

- KMS Lighthouse aligns its data handling practices with the EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).
- Regular data security and privacy reviews are performed to identify risks related to the processing of personal data.
- For details on how we handle personal data, see our Privacy Policy.

Reporting a security concern

To report a security vulnerability or ask a security question, contact support@kmslh.com.