

The Haunted Lighthouse Limited
Security and Compliance Overview
v2.0

1. Overview

The Haunted Lighthouse Limited applies consistent, industry aligned security practices across all consultancy and hosted services. Our approach prioritises privacy, European data sovereignty, data minimisation, and operational resilience. This document outlines our baseline security posture and compliance approach.

2. Security Principles

- Least privilege access enforced across all systems
- Encrypted storage and encrypted backups by default
- Strong authentication using TOTP or WebAuthn for administrative roles
- TLS enforced across all public facing services
- No reliance on non EEA content delivery networks
- Restricted traffic flows through firewalls and service isolation

3. Infrastructure Security

- Bare metal hosting within the European Economic Area
- Hardened operating system configurations
- Regular operating system and application updates
- Service isolation using systemd, containers, or both
- SSH key based access only with password authentication disabled
- Optional IP based restrictions for administrative interfaces

4. Data Protection and GDPR Alignment

- All data stored exclusively on EEA based infrastructure
- Encrypted backups using strong, modern cryptography
- Optional data processing agreements available on request
- No transmission of data to third country processors
- Data minimisation integrated into system design

5. Backup and Recovery Security

- Nightly encrypted backups for managed services
- Off site encrypted backup retention
- Regular verification of backup integrity
- Defined and tested disaster recovery procedures
- Controlled restoration to compliant European hardware

6. Monitoring and Incident Response

- Active service monitoring and health checks
- Optional alerting via email or secure messaging
- Manual review of logs and critical event patterns
- Defined incident response and escalation procedures

7. Client Responsibilities

- Maintain secure client side devices and access controls
- Protect administrative accounts using TOTP or WebAuthn
- Apply role based access controls and moderation practices
- Notify The Haunted Lighthouse Limited promptly of suspected incidents

8. Next Steps

Clients seeking enhanced security or compliance support may request platform specific risk assessments, GDPR guidance for self hosted deployments, backup and disaster recovery alignment reviews, or documentation and policy development.

9. Contact

Email: contact@haunted.lighthouse.co.im

Web: <https://haunted.lighthouse.co.im/consultancy>