Helm Compliance – Security Policy

Regulatory Compliance SaaS (HelmHub) Last updated: February 2026

1. Purpose and Scope

This Security Policy describes how Helm Compliance (“we”, “us”, “our”) protects the security of the HelmHub regulatory compliance software-as-a-service platform, the data processed through it, and the infrastructure on which it runs. It is aligned with UK and international standards including the UK GDPR, ISO/IEC 27001:2022, and good practice for AWS-hosted SaaS. Scope: The HelmHub application (backend, frontend, evidence and reports storage), supporting infrastructure (including Amazon Web Services), and related sub-processors (e.g. payment and communications providers). Audience: Customers, regulators, and auditors who need assurance over our security posture. This policy is published for transparency and forms part of our commitment to regulated UK and global standards.

2. Governance and Responsibilities

- Information security governance is owned at senior level. Roles and responsibilities for security (including access to production systems and sensitive data) are defined and documented. - Privileged roles within the application (e.g. Super User, Organisation Administrator) are assigned only to authorised individuals; access is reviewed periodically and removed when no longer required. - Security-related decisions (e.g. access control, cryptography, incident response) follow this policy and any associated procedures.

3. Access Control and Identity Management

- Authentication: Access to the Service requires authentication. We use industry-standard mechanisms (including JWT-based access and refresh tokens) with appropriate token lifetimes (e.g. short-lived access tokens, limited refresh token validity). - Passwords: User passwords are hashed using a strong, salted algorithm (e.g. bcrypt) before storage. Plaintext passwords are not stored or logged. - Identity and roles: User identity and role (e.g. Organisation Admin, Compliance Manager, Auditor, Consultant) are enforced so that users can access only the data and functions appropriate to their role. - Organisation segregation: Customer data is segregated by organisation. Users cannot access data belonging to other organisations except where explicitly permitted (e.g. consultants assigned to an organisation, or Super User administrative functions). - Licence and status checks: Access to the Service is conditional on a valid subscription and active organisation status; these checks are enforced before use. We implement access control and identity management in line with ISO/IEC 27001 Annex A controls A.5.15–A.5.18 (access control, identity management, authentication information, access rights).

4. Cryptography and Key Management

- Encryption in transit: All access to the Service over the internet is via TLS (HTTPS). We do not serve the application over unencrypted HTTP for production use. - Passwords: Stored using a strong one-way hash with salt; we do not use reversible encryption for passwords. - Integrity: Where appropriate (e.g. audit logs), we use cryptographic mechanisms (e.g. SHA-256) to protect the integrity of data and to support tamper detection. - Secrets and keys: Application and service secrets (e.g. JWT signing keys, API keys, database credentials) are not stored in source code. In production, we use secure configuration and, where applicable, a dedicated secrets store (e.g. AWS Secrets Manager or equivalent). Access to secrets is restricted and reviewed. - Key rotation: Where supported, we follow procedures for periodic rotation of cryptographic keys and secrets in line with risk and vendor guidance. This aligns with ISO/IEC 27001 A.5.10 (use of cryptography) and good practice for key management.

5. Audit Logging and Monitoring

- Audit trail: The Service records security-relevant events, including: authentication (e.g. login), creation, read, update, and delete operations on key entities, export and execution actions, approval/rejection workflows, configuration changes, user lifecycle events, and billing-related actions where relevant. - Log content: Log entries include, where applicable: user

identifier, username, role, timestamp, action, entity type and identifier, description, and (where available) IP address and user agent. Sensitive data (e.g. passwords) are excluded from logs. - Integrity: The audit trail is protected against tampering (e.g. via cryptographic hashing and chain integrity verification). Integrity can be verified for a given organisation and time range. - Retention: Audit logs are retained in accordance with our data retention policy and applicable law. Retention periods and secure deletion are documented. - Access to logs: Access to audit logs is restricted to authorised roles and used for security, compliance, and support purposes only. This supports ISO/IEC 27001 A.5.34 (audit logging) and regulatory expectations for accountability and traceability.

6. Data Classification and Information Handling

- Classification: We apply a defined classification scheme to information (e.g. internal, confidential, regulatory/customer data). Customer data and audit logs are treated as confidential and handled in line with that classification. - Multi-tenancy: Customer data is logically and physically segregated by organisation. Evidence, reports, and other stored artefacts are scoped by organisation (e.g. via organisation-specific storage paths or keys). - Processing: Data is processed only for the purposes of providing and supporting the Service, in accordance with our Terms of Service and Privacy Policy, and in compliance with applicable data protection law (including the UK GDPR and, where relevant, the EU GDPR).

7. Secure Development and Change Management

- Secure development: We integrate security into the software development lifecycle. This includes security-conscious design, code review, and use of secure coding practices. Third-party dependencies are managed and monitored for known vulnerabilities where practicable. - Testing: Testing includes functional, integration, and where appropriate security-relevant tests (e.g. authentication, authorization, input validation, audit logging). - Change management: Changes to the Service and supporting systems follow a defined change process. Deployments use automated pipelines (e.g. CI/CD); feature flags and phased rollouts are used where appropriate. Production changes are controlled and documented. - Environments: Development, test, staging, and production environments are separated. Production data is not used in non-production environments; test data is synthetic or anonymised where possible. This aligns with ISO/IEC 27001 A.5.25, A.5.26, A.5.28, A.5.29, A.5.32 (SDLC, application security, secure coding, security testing, change management) and A.5.31, A.5.33 (separation of environments, test data).

8. Infrastructure and Hosting (AWS)

- Cloud provider: The Service is hosted on Amazon Web Services (AWS). We use AWS regions and services in line with our data residency and resilience requirements (e.g. UK or other designated regions where specified). - Security responsibilities: We follow the AWS shared responsibility model: AWS is responsible for the security of the cloud (physical and infrastructure); we are responsible for the security of our workloads, configuration, data, and access management within the cloud. - Network and configuration: We apply network and configuration hardening (e.g. firewalls, security groups, private subnets where appropriate) and restrict administrative and database access to authorised systems and identities. - Backup and recovery: Backups of critical data and configuration are taken in accordance with our backup and business continuity procedures. Recovery time and recovery point objectives are defined and tested where appropriate. Physical security of data centres is addressed by AWS and documented in AWS compliance programmes (e.g. ISO 27001, SOC 2).

9. Sub-processors and Third Parties

- Sub-processors: We use sub-processors (e.g. cloud infrastructure, payment processing, email, and where applicable AI or other service providers) to operate the Service. Sub-processors are selected with regard to security, privacy, and compliance; we maintain a list of key sub-processors and ensure appropriate contracts and safeguards (e.g. data processing terms, confidentiality) are in place. - International transfers: Where data is transferred outside the UK/EEA, we implement appropriate safeguards (e.g. adequacy decisions, standard contractual clauses) as required by UK and applicable data protection law.

10. Incident Response and Reporting

- Security events: We have procedures for detecting, reporting, and responding to security incidents (e.g. unauthorised access, data breach, service compromise). This includes containment, assessment, notification, and post-incident review. - Customer notification: In the event of a personal data breach that is likely to result in a risk to the rights and freedoms of individuals, we will notify the relevant supervisory authority and affected customers in accordance with applicable law (including UK GDPR breach notification requirements). - Availability: We aim to maintain high availability of the Service; planned maintenance and significant outages are communicated where appropriate. This supports ISO/IEC 27001 A.8.8 (information security event reporting) and regulatory breach notification obligations.

11. Data Retention and Deletion

- Retention: We retain personal data and other customer data only for as long as necessary to provide the Service, fulfil our legal and contractual obligations, and as set out in our Privacy Policy and data retention policy. - Deletion: On termination of a subscription or at the end of the retention period, we delete or anonymise data in accordance with our procedures and applicable law. Customers are responsible for exporting any data they need before termination.

12. Compliance and Review

- Compliance: This policy is designed to support compliance with UK and international standards and regulations relevant to our Service, including but not limited to the UK GDPR, ISO/IEC 27001:2022, and good practice for SaaS and cloud security. - Reviews: This Security Policy is reviewed periodically and updated as necessary to reflect changes in the Service, risk, or legal and regulatory requirements. Material changes will be communicated as appropriate (e.g. via our website or notification to customers).

13. Contact

For questions about this Security Policy or to report a security concern, please contact us: - Email: support@helmcompliance.com - Website: www.helmcompliance.com - Security concerns: Please use the same contact details; we will acknowledge and handle reports in line with our incident response procedures. Document version: 1.0 | February 2026 | Helm Compliance