Hub Hosting – Security & Compliance

Version: HH-SCS-v2025.4

Date: 3 November 2025

Official Legal Contact: support@hub-hosting.com

PREAMBLE

This Security & Compliance Statement ("Statement") outlines Hub Hosting's commitment to maintaining high standards of information security, privacy, and regulatory governance. It reflects our alignment with recognized international frameworks, including ISO/IEC 27001:2022, ISO/IEC 27035:2023, NIS2 Directive (EU 2022/2555), SOC 2 Type II, SOC 3, CIS Controls v8, and applicable Irish and EU legislation.

1. SCOPE OF APPLICATION

This Statement applies to all Hub Hosting operations, systems, facilities, and personnel involved in the delivery of hosting, VPS, domain, and managed services. It covers all data centers and cloud infrastructure operated within the European Economic Area (EEA).

2. GOVERNANCE FRAMEWORK

Hub Hosting maintains an Information Security Management System (ISMS) designed in alignment with the principles of ISO/IEC 27001:2022. Governance is established through documented policies covering risk management, access control, data protection, business continuity, and regulatory compliance. The ISMS is reviewed annually by senior management and subject to internal security and compliance assessments.

3. FRAMEWORKS AND STANDARDS

Hub Hosting's security and compliance framework is based on internationally recognized standards and best practices:

- ISO/IEC 27001:2022 – Information Security Management System principles.
- ISO/IEC 27035:2023 – Incident Response and Security Event Management guidelines.
- NIS2 Directive (EU 2022/2555) – Cybersecurity and network resilience.
- SOC 2 Type II and SOC 3 – Data security and service availability controls.
- CIS Controls v8 – Implementation of essential cybersecurity controls.
- GDPR (EU 2016/679) and Irish Data Protection Act 2018 – Data protection and privacy governance.

4. INFORMATION SECURITY CONTROLS

Hub Hosting implements a defense-in-depth security architecture with administrative, technical, and physical safeguards. Core controls include:

- Risk-based security management and continuous monitoring.
- Network segmentation, encryption, and intrusion prevention.
- Patch management and vulnerability remediation.
- Incident response, audit logging, and configuration management.
- 24/7 data center surveillance and access control.

5. ACCESS CONTROL & AUTHENTICATION

Access to systems and client data is strictly managed through multi-factor authentication (MFA), role-based access control (RBAC), and the principle of least privilege. Administrative access is logged, reviewed, and periodically revalidated.

6. NETWORK & INFRASTRUCTURE SECURITY

Hub Hosting employs enterprise-grade firewalls, intrusion detection and prevention systems (IDS/IPS), DDoS mitigation, and encrypted communication (TLS 1.3). Network activity is continuously monitored, and systems are maintained with current patches and firmware updates to reduce exposure to known vulnerabilities.

7. DATA PROTECTION & PRIVACY

All personal and client data is processed in accordance with GDPR (EU 2016/679) and the Irish Data Protection Act 2018. Data is hosted exclusively within the EEA and encrypted both in transit (TLS 1.3) and at rest (AES-256). Hub Hosting maintains Data Processing Agreements (DPAs) with all subprocessors to ensure privacy and regulatory alignment.

8. INCIDENT MANAGEMENT & REPORTING

Hub Hosting operates a formal Incident Response Procedure (IRP) aligned with ISO/IEC 27035 and the NIS2 Directive. Security incidents are logged, triaged, and escalated through defined workflows. Significant incidents trigger notification to affected clients and, when required, to competent authorities such as the Irish National Cyber Security Centre (NCSC) or Data Protection Commission (DPC) within 24–72 hours.

9. BUSINESS CONTINUITY & DISASTER RECOVERY

Hub Hosting maintains Business Continuity (BCP) and Disaster Recovery (DRP) plans aligned with industry best practices. These plans are reviewed and tested annually. Defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) support service-level commitments and operational resilience.

10. ROLES & RESPONSIBILITIES

The Data Protection Officer (DPO) and Chief Information Security Officer (CISO) oversee all information security and privacy governance activities. All employees receive annual training on cybersecurity, privacy, and ethical conduct. Security roles and responsibilities are defined within the ISMS governance structure and are subject to review during internal audits.

11. LEGAL & REGULATORY COMPLIANCE

Hub Hosting ensures compliance with applicable frameworks and legislation, including:

- GDPR (EU 2016/679) and DPA 2018 (Ireland).
- NIS2 Directive (EU 2022/2555).
- ISO/IEC 27001:2022 and ISO/IEC 27035:2023 principles.
- SOC 2 Type II / SOC 3 trust criteria.
- CIS Controls v8.
- Consumer Rights Act 2022 (Ireland).

Compliance is verified through internal risk assessments, policy reviews, and external audits by independent experts when applicable.

12. GOVERNING LAW & JURISDICTION

This Statement is governed by the laws of Ireland and applicable European Union regulations. Any disputes arising under this Statement shall be subject to the exclusive jurisdiction of the courts of Cork, Ireland.