Security & Compliance Statement

Version: SC-2026.1

Effective Date: 10.02.2026

Issued by: Hub Hosting

Contact: support@hub-hosting.com| legal@hub-hosting.com

Jurisdiction: Ireland / European Union

1. Scope of Application

This Statement applies to all infrastructure, personnel, systems, and operations involved in delivering our:

- Fully managed hosting services
- Managed VPS environments
- Managed cloud storage
- Domain registration services

It covers all data centers and cloud infrastructure operated within the **European Economic Area (EEA)** and any subcontracted subprocessors operating within **adequate jurisdictions** under GDPR.

2. Governance and ISMS Framework

Our internal security governance is anchored in a formal **Information Security Management System (ISMS)** based on **ISO/IEC 27001:2022**. The ISMS includes documented policies for:

- Risk assessment and mitigation
- Access management and control
- Business continuity and disaster recovery
- Data protection and privacy
- Incident response and escalation
- Compliance monitoring

The ISMS is reviewed annually by executive leadership and subject to internal audits and external expert assessments where applicable.

3. Regulatory and Industry Standards Alignment

Our security posture and compliance operations are aligned with the following:

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

4. Information Security Controls

We employ a **defense-in-depth architecture** with the following integrated safeguards:

- Risk-based security controls and continuous monitoring
- Network segmentation and secure architecture
- TLS 1.3 encryption for data in transit; AES-256 for data at rest
- Intrusion detection and prevention (IDS/IPS)
- Regular vulnerability assessments and patch management
- Change management and secure configuration baselines
- Real-time audit logging and anomaly detection
- 24/7 surveillance and biometric access controls in data centers

5. Access Control and Authentication

Access to production systems and client environments is protected via:

- Multi-Factor Authentication (MFA)
- Role-Based Access Control (RBAC)
- Enforcement of the principle of least privilege
- Periodic access reviews and revalidation
- Session logging and tamper-proof access logs

All administrative access is logged and monitored by our security team.

6. Network and Infrastructure Security

We leverage enterprise-grade technologies for perimeter and internal protection, including:

- Firewalls
- DDoS mitigation at the edge
- Intrusion detection and real-time alerting
- Network segmentation and isolation of sensitive systems
- Routine penetration testing and configuration reviews

All hardware and software platforms are regularly updated with verified security patches.

7. Data Protection and Privacy

We fully comply with the **GDPR** and the **Irish Data Protection Act 2018**. Personal data is:

- Stored exclusively within the **EEA** or in **adequate jurisdictions** under GDPR
- Encrypted both in transit (TLS 1.3) and at rest
- Processed only under documented instructions from Clients
- Covered by **Data Processing Agreements (DPAs)** with all subprocessors

Data retention, access, and erasure policies are strictly enforced. Backup and restoration procedures are documented and tested periodically.

8. Incident Management and Reporting

Our **Incident Response Plan (IRP)** is aligned with **ISO/IEC 27035** and **NIS2**, and includes:

- 24/7 incident monitoring and triage workflows
- Severity classification and containment protocols
- Immediate escalation procedures
- Mandatory notification of affected Clients
- Regulatory notification to the **Data Protection Commission (DPC)** or **NCSC (Ireland)** within 24-72 hours, when applicable

All incidents are reviewed post-resolution and entered into continuous improvement processes.

9. Business Continuity and Disaster Recovery

We maintain robust **Business Continuity Plans (BCP)** and **Disaster Recovery Plans (DRP),** which:

- Are reviewed and tested at least annually
- Include clearly defined **Recovery Time Objectives (RTO)** and **Recovery Point Objectives (RPO)**
- Ensure redundancy across data centers and cloud nodes
- Support service continuity in the event of hardware failure, cyberattack, or natural disaster

10. Organizational Roles and Responsibilities

All security, compliance, and privacy functions are overseen by:

- The Chief Information Security Officer (CISO)
- The Data Protection Officer (DPO)

All employees and contractors undergo:

- Annual cybersecurity and privacy awareness training
- Confidentiality and ethics training as part of onboarding
- Background checks in accordance with applicable employment law

Security responsibilities are defined in employee role descriptions and enforced through policy.

11. Continuous Compliance and Verification

Compliance is maintained through:

- Ongoing internal risk assessments
- Scheduled policy and control reviews
- Third-party audits on request or as required by contractual or regulatory obligations

We welcome compliance inquiries and client audits subject to mutual agreement and scope definition.

12. Legal Framework and Jurisdiction

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

13. Contact Information

For compliance, legal, or security-related inquiries, please contact:

Information Security Office

support@hub-hosting.com

legal@hub-hosting.com

dpo@hub-hosting.com

Hub Hosting is a commercial brand owned and operated by the company:

Digital Synergy Ltd

Second Floor, 74 South Mall, T12F3FD Cork, Co. Cork, Republic of Ireland