Hub Hosting - Incident Response Statement

Document ID: HH-IR-ST-v2025.1

Date: 3 November 2025

Official Legal Contact: support@hub-hosting.com

Preamble

Hub Hosting maintains a documented Incident Response Procedure (IRP) aligned with the principles of ISO/IEC 27035:2023 (Information Security Incident Management), the NIS2 Directive (EU 2022/2555), and the General Data Protection Regulation (GDPR – EU 2016/679). This Statement outlines Hub Hosting's commitment to proactive, structured, and transparent handling of information security incidents within its internal Security and Compliance Framework.

1. Purpose and Scope

The purpose of this Incident Response Statement is to publicly outline Hub Hosting's structured and proactive approach to identifying, managing, and mitigating information security incidents. This Statement applies to all hosting environments, systems, infrastructure, and digital services operated by Hub Hosting.

2. Governance and Compliance

Hub Hosting maintains an internal Incident Response Procedure (IRP) aligned with the principles of ISO/IEC 27035 and the NIS2 Directive. The procedure defines roles, escalation paths, and communication workflows to ensure that incidents are addressed promptly, transparently, and in compliance with applicable Irish and EU legislation.

While Hub Hosting is not formally certified under ISO or SOC standards, its security and incident response practices are modelled on international best-practice frameworks to ensure continuous improvement and accountability.

3. 24/7 Security Operations Monitoring

Hub Hosting operates continuous monitoring of infrastructure, network, and hosted environments through automated detection systems, alerting tools, and client reporting channels. Potential incidents are triaged, categorised, and escalated according to severity and potential impact.

4. Incident Classification and Response

Incidents are classified by severity (Levels 1–4) based on their impact on confidentiality, integrity, and availability. The Hub Hosting Incident Response Team (IRT) coordinates containment, investigation, eradication, and recovery actions. Post-incident reviews are conducted to identify root causes, implement corrective measures, and prevent recurrence.

5. Notification and Reporting

In line with GDPR Articles 33 and 34 and the NIS2 Directive, Hub Hosting ensures that any confirmed personal data breach or significant network incident is reported to the Data Protection Commission (Ireland) or other competent authorities within the legally prescribed timeframes. Affected clients are notified transparently when applicable. Internal escalation to the Data Protection Officer (DPO) and senior management occurs within four (4) hours of detection.

6. Annual Review and Testing

The Incident Response Procedure is reviewed and tested at least annually to maintain effectiveness and compliance with evolving regulations. Simulated incident response exercises (“tabletop tests”) are carried out under the supervision of management, the DPO, and Legal Counsel.

7. Contact Information

All suspected or confirmed security incidents, including data breaches or network compromises, should be reported immediately to:

Security Incident Response Team (SIRT)

Email: support@hub-hosting.com