INFORMATION SECURITY AND BUSINESS CONTINUITY POLICY

Revision No: 01   Effective Date: 26.08.2024   Document No: BGİSY-POL-01

1. PURPOSE

This policy aims to ensure the security of information assets and the continuity of critical business processes at H3M Yazılım Danışmanlık Sanayi ve Ticaret A.Ş. In compliance with ISO/IEC 27001:2022 and ISO 22301:2020 standards, it is essential to manage risks, respond to incidents, and maintain preparedness for potential disruptions within the scope of the Information Security Management System (ISMS) and the Business Continuity Management System (BCMS).

2. SCOPE

This policy applies to all employees, interns, consultants, business partners, and third-party service providers. It covers information systems, software, databases, documents, and all operational activities that may affect the company's business continuity.

3. POLICY STATEMENTS

H3M commits to:

- Protecting information assets according to the principles of confidentiality, integrity, and availability,
- Ensuring full compliance with legal regulations, contracts, and customer obligations,
- Identifying, assessing, processing, and mitigating risks to acceptable levels,
- Defining critical business processes and services, and developing and testing business continuity plans to ensure uninterrupted operation,
- Implementing predefined response mechanisms for emergencies, disasters, and information security breaches,
- Continuously monitoring, measuring, reviewing, and improving the performance of ISMS and BCMS,
- Providing information security and business continuity awareness training to all personnel and relevant parties,
- Defining and applying asset ownership, access controls, and monitoring mechanisms,
- Ensuring the sustainability of ISMS and BCMS through executive commitment.

4. MANAGEMENT COMMITMENT

The management of H3M provides necessary resources for the effective implementation of this policy and evaluates information security and business continuity performance through regular management reviews. The policy is reviewed at least once a year or as needed and updated accordingly.

5. RESPONSIBILITIES

- ISMS & BCMS Coordinator: Ensures the implementation and continuity of the policy.
- All Employees: Are obliged to act in accordance with the policy requirements.
- HR and IT Departments: Are responsible for training, access control, and infrastructure management.

6. PUBLICATION AND ACCESS

This policy is communicated to all staff and published on the internal information sharing platform.