Information Security and Privacy Policy

1. Purpose

This policy has been established to protect the confidentiality, integrity, and availability of OneIngage's information assets, and to ensure the security of information belonging to employees, customers, suppliers, and other stakeholders.

2. Scope

This policy applies to all employees, interns, contractors, visitors, and third-party service providers within OneIngage. It covers all physical, electronic, and written information assets.

3. Definitions

- Information Security: Protection of the confidentiality, integrity, and availability of information.

- Confidentiality: Preventing unauthorized access to information.

- Integrity: Ensuring the accuracy and completeness of information.

- Availability: Ensuring authorized users have access to information when needed.

4. Core Principles

- All information assets must be classified and protected with appropriate security measures.

- Legal regulations (KVKK, ISO/IEC 27001, Law No. 6698, etc.) and contractual obligations must be followed.

- Access to corporate networks, systems, and data must be restricted based on roles and permissions.

- All users are required to participate in information security awareness training.

- Information security incidents must be reported immediately in accordance with incident management procedures.

5. Responsibilities

- Senior Management: Responsible for approving the policy, providing resources, and supporting a culture of information security.

- Information Security Officer (IT Manager): Responsible for establishing, maintaining, and improving the information security system.

- All Employees: Responsible for complying with information security policies and reporting suspicious incidents.

6. Physical and Environmental Security

- Entry/exit controls must be in place to prevent unauthorized access, and server rooms must be kept locked.

- Backup and business continuity plans must be implemented to protect against hardware failure, natural disasters, etc.

7. Access Controls

- Each user is granted access only to the systems required for their job responsibilities.

- Password management policies must be enforced; strong passwords and measures such as MFA must be used.

8. Data Security and Privacy

- Personal data is processed and stored in compliance with Law No. 6698 (KVKK) and relevant regulations.

- Data Loss Prevention (DLP) systems and encryption methods are used.

9. Information Security Breaches

- Information security breaches must be reported immediately to the Information Security Officer.

- Each breach is recorded, evaluated, and corrective/preventive actions are implemented as necessary.

10. Policy Review

This policy is reviewed and updated at least once a year and whenever necessary (e.g., due to legislative changes, incidents, or audit results).