# DATA SECURITY POLICY

**Our Mission**

As **REGNUM HOTELS**, we are committed to protecting the confidentiality, integrity, and availability of guest information, employee data, business processes, and other sensitive information. We adopt best practices to prevent information leakage and promote a culture of information security by safeguarding all information assets. Our priority is to ensure customer trust and maintain business continuity through this approach.

**Our Vision**

We aim to create a sustainable security culture by integrating information security into all our processes. With a work environment where information is protected, we strive to continuously improve the quality of our services and operations.

**Our Commitments to Information Security**

- Protection of Information Assets: Identifying, classifying, and implementing appropriate protection measures for information assets based on risk.
- Training and Awareness: Providing regular information security training to employees to raise awareness and foster a culture of security.
- Risk Assessment: Continuously assessing information security risks and taking effective preventive measures.
- Monitoring and Improvement: Regularly reviewing, improving, and auditing our policies, processes, and controls to ensure compliance.
- Incident Management: Identifying, recording, responding to information security incidents, and reporting violations when necessary.
- Legal and Regulatory Compliance: Ensuring full compliance with applicable laws, regulations, and contractual obligations.
- Business Continuity: Ensuring uninterrupted service through effective information security measures.

This policy applies to all employees, interns, outsourced service providers, and third parties using information and systems belonging to REGNUM HOTELS. All parties are obligated to adhere to the principles of information security and fulfill their assigned security responsibilities.

Every employee is responsible for ensuring the confidentiality, integrity, and availability of information. All personnel must comply with the **REGNUM HOTELS Human Resources Regulations**, **Code of Ethics**, and **Personal Data Protection Law (KVKK)**.

REGNUM HOTELS is committed to full compliance with the KVKK and will take all necessary measures to protect personal data.

- **Information Security Managers** are responsible for implementing the policy, organizing necessary training, and guiding the information security processes.
- **IT Manager** ensures the policy is kept up-to-date and establishes an effective management framework against information security risks.
- **Department Managers** are responsible for ensuring the compliance of the processes under their control with the information security policy. In cases of non-compliance, necessary disciplinary actions will be taken, and legal proceedings will be initiated if required.

The policy is reviewed at least once a year and updated as needed.

The **Information Security Management Team** monitors and reports the implementation of the policy. Violations may result in disciplinary action, termination of employment, and legal proceedings.

**Our Goals**

- Ensuring the continuity of information systems.
- Maximizing security compliance through increased employee awareness.
- Achieving full compliance with agreements made with third parties.
- Preventing information security breaches and turning them into learning opportunities.
- Producing, accessing, and storing information in compliance with legal requirements.
- Implementing the most up-to-date technical security measures.

All REGNUM HOTELS employees are responsible for contributing to these goals.