

INFORMATION SECURITY POLICY

At Royal Group Hotels, in line with our innovative, reliable, sustainable and guest-oriented approach to service, we regard the protection of our information assets at every stage of our operations as one of the fundamental elements of our corporate governance.

In order to protect the information of our guests, employees, business partners, suppliers and all other stakeholders, to make information security an integral part of our corporate culture, and to continually improve our information security practices, we commit to:

- **Information Security Management:** Developing our information security processes based on the core principles of the ISO/IEC 27001 standard, and establishing, implementing and continually improving technical, physical and administrative controls to protect our information assets;
- **Confidentiality, Integrity and Availability:** Protecting the confidentiality, integrity and availability of our corporate information assets, and taking the necessary security measures against the risks of unauthorized access, modification, loss, disclosure and misuse;
- **Risk Management:** Systematically identifying, analyzing and evaluating information security risks; defining risk acceptance criteria and risk owners, developing and implementing appropriate controls, and regularly monitoring their effectiveness;
- **Protection of Personal Data:** Processing, storing and protecting the personal data of our guests, employees and business partners in compliance with applicable legislation, in particular the Turkish Personal Data Protection Law No. 6698 (KVKK), and destroying it using legally compliant methods at the end of the statutory retention periods;
- **Legal and Contractual Compliance:** Complying with applicable national and relevant international regulations on information security, related legislation, contractual obligations and the information security requirements of our stakeholders;
- **Digital Security:** Taking the necessary measures to ensure information security across hotel management systems, reservation infrastructures, guest relations applications, payment systems, corporate communication networks and other digital platforms;
- **Access Authorization:** Restricting access to information assets in line with duties, authorities and responsibilities; preventing unauthorized access, regularly reviewing access rights and ensuring that information is accessible only to authorized persons;
- **Protection of Information Assets:** Classifying information assets in electronic and physical environments according to their sensitivity levels, and defining and applying appropriate rules for their storage, sharing, transfer, backup and secure disposal;
- **Business Continuity:** Reducing the potential impact of information security threats on our operational processes and service continuity, and developing measures to support the continuity of critical information systems;
- **Information Security Incident Management:** Detecting and reporting potential information security breaches and cybersecurity incidents in a timely manner, responding to incidents effectively and taking corrective actions to prevent their recurrence;
- **Employee Awareness:** Ensuring that all our employees embrace their information security responsibilities, and fostering a culture of secure information use through training and awareness activities;

- Supplier and Business Partner Security: Defining the information security obligations of our outsourced service providers, suppliers and business partners, and monitoring their compliance with the relevant security requirements;
- Technological Development and Continual Improvement: Keeping our information security practices up to date by following emerging technologies, digital transformation processes and evolving cybersecurity threats, and evaluating and continually improving their performance;
- Corporate Reputation and Trust: Through our information security practices, preserving the trust of our guests and all stakeholders, strengthening our corporate reputation and ensuring the sustainability of our reliable service approach.

We hereby declare our commitment to the principles set out above.

As the Top Management of Royal Group Hotels, we support the implementation of this policy across all facilities, departments and relevant areas of activity within the group, its communication to our employees and relevant stakeholders, the provision of the necessary resources, and the continual improvement of our information security practices through regular review.