MIRAMARE HOTELS
ISO 27001:2022 Information Security Policy

This Information Security Policy has been established to define the security measures related to the information security management system (ISMS) of Miramare Hotels and to ensure full compliance with the ISO 27001:2022 standard. The policy applies to all employees, suppliers, service providers, and other relevant parties, and covers all operations and data processing activities of Miramare Hotels.
Miramare Hotels is committed to establishing an ISMS in accordance with the ISO 27001:2022 standard to manage information security risks, minimize these risks, and create an effective information security culture. The ISMS includes all necessary procedures and controls to identify, monitor, and audit key information security risks.

Information Security Principles:
Miramare Hotels agrees to adhere to the following information security principles:

- **Confidentiality:** Information is accessible only by authorized personnel and protected from unauthorized access by third parties.
- **Integrity:** Information is safeguarded against unauthorized changes and all types of data errors or corruption are prevented.
- **Availability:** : Necessary information is made accessible at all times to authorized users.
- **Legal and Regulatory Compliance:** All information security activities are conducted in accordance with applicable legal regulations and industry standards.

Risk Management: Miramare Hotels conducts ongoing risk assessments for all information assets to identify potential threats and vulnerabilities. Based on these risks, appropriate security measures and control mechanisms are implemented to minimize them. Risk assessments are reviewed regularly and updated as necessary.

Information Security Breaches and Incident Management: Any information security breach or incident is immediately reported to the information security team, and corrective actions are taken to minimize the impact. The incident management process is designed to provide rapid solutions and conduct root cause analyses to prevent recurrence.

Employee Training and Awareness: All employees will be regularly trained on information security policies, procedures, and best practices. Continuous awareness activities will be conducted to increase information security awareness, ensuring employees understand their responsibilities.

Protection of Information Assets: All information assets (data, systems, infrastructures, etc.) will be securely protected and accessible only by authorized individuals. Technical and administrative controls including encryption, backup, and secure data deletion will be in place.

Access Controls: Access is granted solely based on business needs. User access rights are reviewed immediately after role changes or termination, and necessary updates are applied. All accesses will be managed to be traceable and recordable.

Supplier and Third-Party Management: Miramare Hotels ensures that all suppliers and third-party service providers operate in compliance with information security policies. Information security requirements will be explicitly stated in supplier agreements.

Continuous Improvement: Miramare Hotels adopts the principle of continuous improvement for its ISMS. The system's effectiveness is regularly evaluated through internal and external audits, and corrective or preventive actions are taken as needed. Information security performance is constantly monitored and reported.

Information Security Audits and Monitoring: The effectiveness of information security measures will be regularly assessed through internal and external audits. Audits will be conducted in accordance with ISO 27001:2022 requirements, and any non-conformities will be addressed immediately.

Policy Review and Update:
This policy will be reviewed regularly and updated as needed to ensure compliance with current regulations and requirements. Updates to the policy will be approved by senior management.

Responsibilities and Obligations:
All Miramare Hotels employees, managers, and suppliers are responsible for information security. Employees are obligated to comply with information security policies; violations may result in disciplinary action. Senior management oversees the effective implementation of the ISMS and ensures necessary resources are provided.
Miramare Hotels is committed to fulfilling all information security requirements in accordance with the ISO 27001:2022 standard and effectively implementing this policy. Information security is one of the top priorities of the organization, and a secure information environment will be ensured with the contribution of all employees.

GENERAL MANAGER