GALATA WIND ENERJI A.S.
INFORMATION SECURITY POLICY

1. Purpose

As Galata Wind Energy Inc. (**"Galata** Wind" and/or "Company"), we treat information security as a strategic priority within the scope of business continuity and commit to establishing a "reliable, effective, and compliant" information management system that covers all our activities. This policy has been created to ensure the business continuity of our company, comply with legal and regulatory requirements, provide protection against cybersecurity threats, and increase stakeholder confidence.

2. Scope

This Policy covers all Galata Wind employees, business partners, suppliers, service providers, and all parties accessing company networks. All information assets, systems, and digital platforms used, processed, or stored by Galata Wind are covered by this policy.

3. Definitions and Concepts

To clarify the framework of our information security policy for all relevant parties, the basic concepts are defined below:

Senior Management: The decision-making team that determines Galata Wind's strategic direction and is responsible for the organization's overall policies and objectives. Senior management typically consists of the CEO (Chief Executive Officer), Executive Board Members, and managers reporting directly to the CEO. In terms of information security, senior management also refers to the managers designated as responsible for approving the information security policy, overseeing its implementation, providing the necessary resources, setting objectives, and carrying out systematic improvement processes.

Information: Includes all data and documentation in any written, verbal, electronic, or physical medium, regardless of whether it constitutes a trade secret, including Galata Wind's operations, strategic plans, financial data, customer and supplier information, employee data, and intellectual property rights.

Information Assets: Any data, software, system, network, hardware, and documentation used in the company's commercial and operational processes is considered an information asset.

Information Security: Refers to the protection of information within the framework of the principles of confidentiality, integrity, and availability. This approach includes security controls against the risks of unauthorized access, alteration, loss, and destruction.

Confidentiality: This principle ensures that information is accessible only to authorized individuals.

Integrity: Aims to protect the accuracy and reliability of information and prevent unauthorized changes.

Availability: Ensures that information is accessible by authorized persons in a timely manner as required by business processes.

Information as a Corporate Asset: Galata Wind views information as a strategic corporate asset and considers it a critical element for the company's success and business continuity. Therefore, protecting information is not only a technical requirement but also part of corporate risk management.

4. Basic Principles

Our information security management system is managed in accordance with the following objectives and fundamental principles:

- **Confidentiality:** Ensuring that information is accessible only to authorized individuals.
- **Integrity:** To protect the accuracy and reliability of information and prevent unauthorized changes.
- **Accessibility:** Guaranteeing that information is accessible to authorized persons when needed.

5. Information Security Management Model

Galata Wind treats information security **as an integral part of its corporate risk management approach**. **The Information Security Management Model** was created to ensure the Company's business continuity, conduct its operations securely, and provide its stakeholders with a reliable energy infrastructure.

This model covers the processes of determining, implementing, continuously improving, and adopting information security policies throughout the entire organization. Our company views information security not only as a technical issue but also as one of the fundamental elements of our business strategy.

Our Information Security Management Model is based on the following key elements:

Leadership and Commitment: Includes senior management's responsibility and support for information security.

Risk Management: Identifying threats to information assets and managing them by integrating control mechanisms into the company's risk management.

Information Security Culture: Increasing the awareness of employees, business partners, and suppliers regarding information security.

Information Security Team: This is the technical and managerial team responsible for protecting Galata Wind's information assets, taking precautions against cyber threats, managing information security systems, and continuously improving them.

Continuous Improvement: The development of information security practices through systematic audits and reviews.

5.1. Leadership and Commitment

Galata Wind's senior management **demonstrates active leadership** in establishing, implementing, and continuously improving information security policies. **Information security is not considered merely a technical detail managed by the Information Technology departments, but rather a critical issue in terms of corporate governance and sustainable business strategy.**

Our company's approach to leadership and commitment in information security is shaped by the following principles:

5.1.1. Information Security as a Strategic Priority

- The Galata Wind Board of Directors **considers information security to be one of the fundamental elements of business continuity and operational efficiency.**
- Information security is seen as **a critical element in ensuring the uninterrupted operation of renewable energy infrastructure and digital operations**.
- Proactive approaches are developed against cybersecurity threats to minimize potential attacks on the company's energy production processes.
- Information security investments **are integrated with the company's overall risk management and sustainability policies.**

5.1. 2. Providing Resources and Support

- **Financial, technical, and human resources are allocated** to support information security.
- The Galata Wind Management and Executive Board works in coordination with relevant departments to ensure the applicability of information security policies.
- **Information security teams are authorized by senior management and provided with access to the necessary resources.**
- **Senior management** provides the necessary support for updating **the technological infrastructure**, developing data protection systems, and organizing security training for employees.

5.1. 3. Information Security Awareness in Company Culture

- **To strengthen the information security culture**, senior management establishes regular communication with each unit of the Company and communicates requests and objectives.

- **Training and awareness campaigns** aimed at increasing employee awareness of information security **are encouraged**.
- **It is emphasized that** each employee **is individually responsible for information security**.
- **Executive Board Members and department managers** set goals that indicate they value a work culture that complies with information security standards.

5.1. 4. Responsibility and Accountability

- Senior management **holds regular review meetings** to assess the effectiveness of information security practices and identify areas for improvement.
- Accountability mechanisms are established for **the management of issues directly related to information security**.
- Senior management adopts **a zero-tolerance approach to information security breaches** and follows the necessary disciplinary processes.

5.1. 5. Legal Processes and Compliance

- Galata Wind **commits to full compliance with ISO 27001, KVKK, GDPR (General Data Protection Regulation), and industry regulations**.
- Information security processes are managed in line with **the digital risk management expectations of the CSRD**.
- Galata Wind **encourages participation in external audit and certification processes** in order to comply with legal requirements and implement best practices.

5.1.6. Continuous Improvement and Innovation

- **Data-driven analyses and performance measurements are conducted** to enhance the effectiveness of information security systems.
- **Cyber threat intelligence and new technologies are monitored, and** information security policies are continuously updated.
- **Security principles are prioritized in digital transformation processes**, and innovative solutions are integrated into the process.

6. Responsibilities

At Galata Wind, information security is not solely the responsibility of one department or the IT team, but rather the shared responsibility of all company employees and managers.

While senior management is responsible for establishing, directing, and providing resources for information security strategies, the Information Security Team manages the implementation of these strategies, conducts risk assessments, and ensures the continuous improvement of security controls.

Employees are responsible for complying with security policies, participating in awareness training, and reporting suspicious activities to protect information assets.

Internal audits are conducted regularly to ensure the effectiveness of information security processes. Third-party service providers and business partners are also responsible for complying with defined security requirements.

7. Effective Date

This Policy was approved by the Galata Wind Energy Inc. Board of Directors on ...../...../2025 with decision number 2025/..... It will be reviewed and updated as necessary.

8. Additional Procedures

This policy establishes the general framework for Galata Wind's information security management. However, implementation details and operational requirements are defined in the relevant procedures. Employees, contractors, and third parties must act in accordance with the following procedures to ensure full compliance with information security processes. Current procedures are accessible via the Galata Wind intranet system or the Information Security Department.

1. Information Security Risk Management Procedure

2. Access Control Procedure

3. Data Classification and Protection Procedure

4. Password Management and Authentication Procedure

5. Physical Security and Data Center Access Procedure

6. Information Security Incident Management and Breach Notification Procedure

7. Business Continuity and Disaster Recovery Procedure (Disaster Recovery Plan - DRP)

8. Supplier and Third-Party Security Procedure

9. Employee Information Security Awareness and Training Procedure

10. Cyber Threat Intelligence and Proactive Security Measures Procedure

11. Cloud Security Procedure