1. PURPOSE

With its Information Confidentiality, Information Security, and Digitalization Policy, SUB IQ YAZILIM ÇÖZÜMLERİ TİCARET LİMİTED ŞİRKETİ (SUB IQ) aims to:

- **Meet the requirements of the ISO 27001:2022 Information Security Management System,**
- **Sustain improvement activities,**
- **Monitor compliance with laws and regulations,**
- **Fulfill information security requirements by analyzing risks and opportunities, and**
- **Integrate new-generation technologies into business processes by following the latest developments in digitalization.**

---

2. SCOPE

All employees, suppliers, group companies, and business partners of SUB IQ are required to fully comply with our Information Confidentiality, Information Security, and Digitalization Policy. Any action contrary to the principles outlined in this policy is considered an information security breach and is subject to ethical evaluation and disciplinary action.

This policy is regarded as an integral part of the following:

- **Ethics, Compliance, and Disclosure Policy,**
- **Anti-Bribery and Anti-Corruption Policy,**
- **Responsible Procurement and Supply Chain Policy,**
- **Integrated Management System Policy,**
- **Sustainability Policy.**

---

3. INFORMATION CONFIDENTIALITY AND SECURITY

3.1 Information Access

All technologies, products, and data related to customers, suppliers, or group companies owned by SUB IQ must be accessible only to authorized personnel. Individuals without authorization may not access this data without approval from the Board of Directors. If an employee needs access to data outside their area of authorization, they must obtain approval from the Board.

3.2 Behaviors Considered as Breach of Confidentiality and Security

The following actions are deemed violations of information confidentiality and security:

- **Leaking or using any personal data for personal gain,**

- **Using internal confidential information for non-business purposes or sharing it with third parties,**
- **Removing proprietary technological infrastructure, designs, or software from the company,**
- **Disclosing internal data to be used for stock trading or to gain material/immaterial benefit,**
- **Attempting to or successfully bypassing the company's access controls,**
- **Concealing known vulnerabilities in our systems,**
- **Accessing information outside of one's authority without permission,**
- **Using customer data without consent,**
- **Requesting customer data beyond what is necessary for operational processes,**
- **Introducing malicious software into company systems,**
- **Causing data leaks due to weak password usage,**
- **Sharing system passwords with consultants without a confidentiality agreement,**
- **Unauthorized destruction of physical documents,**
- **Attempting to access information through fake emails or websites.**

3.3 Our Information Security Measures

- **Network access is restricted per individual; access is defined through address-based mapping.**
- **Access filtering rules are applied by department and user level.**
- **Data is protected from external access through a strong VPN infrastructure.**
- **Email security is maintained by internationally recognized providers.**
- **Department-specific storage areas are designated; data access is granted only to authorized department personnel.**
- **National and international information security systems are closely monitored and reinforced.**
- **Risks related to information security are regularly analyzed by our IT specialists.**

3.4 Rules for Using SUB IQ Information Systems
Users of our information systems must:

- **Take precautions against identified risks as determined by IT specialists,**
- **Read and internalize the "Ethics, Compliance, and Disclosure Policy", the "Information Confidentiality, Information Security, and Digitalization Policy", and the "Anti-Bribery and Anti-Corruption Policy",**

- **Use the information systems in compliance with applicable laws, internal policies, business ethics, and professional conduct,**
- **Refrain from using or disclosing company information for personal gain,**
- **Maintain the confidentiality of all supply chain partners, group companies, and business partners,**
- **Access corporate information resources only when required by their job responsibilities.**

3.5 Third Parties

Consultants or third parties using our information systems must operate in alignment with our policies. When third-party access is necessary, the following rules apply:

- **Company data and assets may not be shared without permission,**
- **No voice, video recordings, or photographs may be taken without prior approval,**
- **Data or software may not be copied without explicit consent,**
- **Services performed on company premises must be supervised by the IT department.**

---

4. DIGITALIZATION

SUB IQ's digitalization efforts aim to:

- **Build robust systems,**
- **Strengthen existing structures through technology,**
- **Eliminate risks related to time, cost, and security,**
- **Improve operational efficiency, and**
- **Deliver higher-quality services to customers.**

4.1 Expectations from Our Employees Regarding Digitalization

- **Employees must follow new and emerging technologies closely,**
- **Identified technological opportunities must be reported to senior management with integration suggestions,**
- **Employees should internalize knowledge to use technological infrastructure fully and efficiently,**
- **Customer services should be delivered completely, accurately, and promptly using our technological infrastructure,**
- **Technical issues must be promptly reported to the IT department for resolution.**

4.2 Providing Digital Conditions to Our Employees

- **The company offers employees the most modern and efficient technological infrastructure for productive and comfortable work,**
- **Provides a strong and reliable infrastructure to ensure information confidentiality and security,**
- **Maintains uninterrupted electronic communication channels for employees, suppliers, partners, and group companies,**
- **Operates 24/7 open notification channels for reporting violations, feedback, requests, and complaints. Any stakeholder can submit their reports at any time.**

Date: 01.01.2025
Chairman of the Board of Directors, SUB IQ: Yusuf Yiğit AKKUŞ

Signature: