ISMS Policy

1. İÇDAŞ Inc. ISMS POLICY

İÇDAŞ BGYS politikası ile kurumsal güvenilirliğini ve temsil ettiği markanın imajını korumayı, üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamayı, firmamızın temel ve destekleyici işfaaliyetlerinin en az kesinti ile devam etmesini sağlamak amacıyla, bilişim hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziksel ve elektronik bilgi varlıklarının bilgi güvenliğini sağlamayı ve üst yönetimin bilgi güvenliği yaklaşımını tüm çalışanlara ve ilgili taraflara bildirmeyi hedefler.

İÇDAŞ, Üst yönetim tarafından onaylanmış bu politika ile “BGYS Hedefleri” dokümanında belirtilen hedeflere ulaşmak için aşağıdaki ilkeleri benimser:

- To protect information against unauthorized access and reduce the number of detected unauthorized access incidents
- To ensure the confidentiality of information and minimize incidents such as disclosure of confidential information
- To prevent the intentional provision of information to unauthorized persons
- To ensure the integrity of information and reduce the number of integrity-related violations
- To ensure the availability of information and maintain uptime rates at levels appropriate to business needs
- To meet the requirements of applicable laws and contracts, and to minimize legal sanctions and contractual non-compliance issues
- To provide information security training to all employees and ensure that all information security vulnerabilities and suspected weaknesses are reported to responsible parties, minimizing the number of unreported incidents

- To prevent attacks against systems and maintain the number of successful attacks at zero
- To ensure that processes within scope continue with minimal interruption and keep total downtime below one day per year

İÇDAŞ declares that the implementation and monitoring of the “Information Security Policy,” as well as the enforcement of necessary sanctions in the event of security violations, are supported by management.

İÇDAŞ ensures the confidentiality, integrity and availability of information to enable timely, complete, accurate and uninterrupted access to its information assets, thereby maintaining integrity in its business relationships with customers and suppliers, achieving competitive advantage and safeguarding its corporate reputation.

İÇDAŞ supports its ISMS with an ISMS Manager and team, whose duties and responsibilities are defined in the “Information Security Organization Policy,” in order to manage the confidentiality, integrity, and availability of corporate information and to maintain the security of corporate information and information systems that are accessed, processed, transmitted, or managed by external parties.

The risk management framework includes the identification, assessment, and treatment of information security risks. Risk assessment, the Statement of Applicability, the risk treatment plan, and how information security risks are controlled are defined in the “Risk Management Policy.” The ISMS Manager is responsible for the management and implementation of this policy.

Rather than completely eliminating risks, the “Risk Management Policy” is applied to reduce the likelihood of undesirable events, minimize their impact, define acceptable risk levels, and make decisions regarding residual risks. This policy and its processes define a systematic method for analysis, improvement, and monitoring of risks.

İÇDAŞ supports the prevention of unauthorized physical access to its premises and information, unauthorized entry, loss, damage, theft, compromise of organizational assets, and disruption of business processes through its “Physical and Environmental Security Policy.”

İÇDAŞ aims, through its “Information Security Incident Management Policy,” to define roles and responsibilities regarding the detection, analysis, and response to security incidents that may occur in information systems, and to ensure that incidents are handled quickly and accurately.

İÇDAŞ supports the “Business Continuity Policy” to reduce the impact of long-term failures or disasters that may occur in information systems on critical business processes and to ensure that operations can resume from the point of interruption within a short time.

İÇDAŞ supports the “Operations and Communications Management Policy” to ensure that information assets are operated correctly and securely, to minimize damage that may arise due to system errors, to protect the confidentiality, integrity, and availability of assets, and to define the rules that must be followed for secure network communications within İÇDAŞ’s areas of responsibility.

İÇDAŞ supports compliance of all employees with security policies, laws, regulations, contracts, and security requirements, and addresses violations through its “Compliance Policy.”

ISMS Policy

İÇDAŞ defines the necessary security requirements through its “Human Resources Security Policy” to prevent damage to or destruction of information assets caused by intentional actions, misuse, or improper use by employees, subcontractors, consultants, or third parties..

Through its “Asset Management Policy,” İÇDAŞ aims to ensure the confidentiality, integrity, and availability of its information assets, to manage them effectively and efficiently, and to ensure their controlled use. These assets are categorized as information, software, hardware, people, services, and processes.

İÇDAŞ aims to implement an “Access Control Policy” stating that physical and logical access to corporate information assets may only be performed by authorized persons and devices.

To regulate the principles and rules for protecting the confidentiality, integrity, and availability of information during the use of corporate information systems and services — including but not limited to email, intranet, extranet, internet, and all other electronic communication methods and technologies — as well as computers, mobile phones, handheld devices, navigation devices, fax machines, photocopiers, and similar equipment assigned exclusively for business purposes under employment contracts, İÇDAŞ establishes its rules and employee obligations under the “Acceptable Use Policy.”

İÇDAŞ aims, through its “Information Systems Acquisition, Development, and Maintenance Policy,” to ensure that security becomes an integral part of the lifecycle of information systems acquisition, development, and maintenance.

2. İLİŞKİLİ POLİTİKA ve DOKÜMANLAR

- Risk Management Policy
- Information Security Organization Policy
- Asset Management Policy
- Human Resources Security Policy
- Physical and Environmental Security Policy
- Operations and Communications Management Policy
- Access Control Policy
- Information Systems Acquisition, Development and Maintenance Policy
- Information Security Incident Management Policy
- Business Continuity Policy
- Compliance Policy
- ISMS Scope Statement
- ISMS Objectives Document

3. DOKÜMAN SAHİBİ

ISMS Management

4. REVİZYON ve GÖZDEN GEÇİRME

İÇDAŞ management is responsible for supporting information security initiatives by providing adequate resources and for periodically reviewing the effectiveness of implemented security controls. Detailed ISMS roles and responsibilities are defined in the Information Security Organization Policy.

5. TANIMLAR

Information Security Management System (ISMS):

Part of the overall management system, based on a business risk approach, used to establish, implement, operate, monitor, review, maintain, and continually improve information security.

Information Security:

Preservation of the confidentiality, integrity, and availability of information. In addition, it includes properties such as authenticity, accountability, non-repudiation, and reliability. (ISO/IEC 27001)

Management:

ISMS Managers appointed by Senior Management.

Senior Management:

The General Manager and Executive Board to whom ISMS Management reports.

Information Asset:

Assets owned by İÇDAŞ that are necessary for maintaining uninterrupted business operations and are therefore required to be protected.

ISMS Policy

Confidentiality:

The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Integrity:

The property of safeguarding the accuracy and completeness of assets.

Availability:

The property of being accessible and usable upon demand by an authorized entity.

Board of Directors

20.05.2026