1. PURPOSE:

The purpose of the Information Security Policy is to define the basic information security principles of DATACOSMOS.

2. SCOPE:

The scope of the Information Security Policy includes all organizations and information assets.

3. RESPONSIBILITIES:

3.1. Top Management
Responsible for ensuring that the Information Security Policy meets the needs of the institution, providing the necessary support and oversight for its implementation, and reviewing the policy at least once a year or when situations requiring changes in the policy arise.

3.2. ISMS & ITSM Coordinator
Responsible to top management at every stage from the establishment to the operation and management of the Information Security Management System.

3.3. ISMS Coordination Team
The ISMS coordination team, appointed by top management, is responsible for ensuring that the Information Security Policy meets the needs of the institution, providing the necessary support and oversight for its implementation, and reviewing the policy at least once a year or when situations requiring changes in the policy arise.

3.4. All Personnel
Responsible for fulfilling the requirements of the Information Security Policy as required by their job duties.

4. DEFINITIONS:

ISMS: Information Security Management System
Confidentiality: Ensuring that information is accessible only to those authorized to have access.
Integrity: Safeguarding the accuracy and completeness of information and processing methods.
Availability: Ensuring that authorized users have access to information and associated assets when required.

5. APPLICATION:

5.1. Information Security Policy

Mission:
To provide the highest quality solutions for data management at every stage as a System Integrator with knowledge, experience, and trust. To evaluate needs with a knowledge-based and solution-oriented approach, and to implement reliable and manageable projects compatible with evolving technology. To ensure the continuity of solutions for corporate customers with consulting, support, and training services provided by Datacosmos's own resources, ensuring lasting satisfaction.

Vision:
To become a preferred, leading, and reliable system integrator in the upper corporate market in Turkey & Middle East, creating a difference with the solutions we offer and the services provided by our own resources, based on our years of experience and knowledge.

ISMS Policy

● Manage information assets, determine the security values, needs, and risks of these assets, and develop and implement controls for security risks.
● Define the framework that determines methods for identifying information assets, their values, security needs, vulnerabilities, threats to assets, and the frequency of these threats.
● Define a framework for assessing the impact of threats on the confidentiality, integrity, and availability of assets.
● Establish working principles for processing risks.
● Continuously monitor risks by reviewing technological expectations within the scope of the service provided.
● Ensure compliance with national or international regulations, legal and relevant legislative requirements, contractual obligations, and company responsibilities to internal and external stakeholders related to information security.
● Reduce the impact of information security threats on service continuity and contribute to continuity.
● Be competent to quickly respond to potential information security incidents and minimize the impact of incidents.
● Maintain and improve the level of information security over time with a cost-effective control infrastructure.
● Provide all personnel with awareness, information, and training on Information Security Management System Policies, Processes, etc. Repeat this training at regular intervals.
● Continuously improve the system by considering the results of applications, audits, and corrective actions within the scope of the Information Security Management System.
● Conduct the Information Security Management System in an integrated manner with other management systems within the company.
● Work to understand and meet the requirements of the Personal Data Protection Law (PDPL).
● Continue efforts to ensure environmental sustainability and awareness of environmental and social responsibility in response to climate change.

● Pay attention to using environmentally sensitive and recyclable products within the scope of activities.

● Enhance the company's reputation and protect it from adverse effects based on information security.

General Manager
28.06.2024