IMS.IT[EN] Information security policy

Document reference

INTEGRATED MANAGEMENT SYSTEM	
Policy	
Ref:	IMS.IT[EN] Information security policy
Version:	2.1

Revision history

Date	Version	Author	Change details
05.01.2018	1.0	Vladislav Nikitin	The final version is prepared.
11.03.2022	1.1	Vladislav Nikitin	The policy is aligned with the Company's vision and strategy.
29.05.2023	1.2	Vladislav Nikitin	The document reference was updated.
01.04.2023	2.0	Vladislav Nikitin	The policy has been aligned with an integrated management system approach. The document reference has been changed.
17.07.20	2.1	Ayvar Fedulov	The term "personnel" has been introduced.

Table of contents

1. Introduction

As a trusted vendor and responsible employer, Itransition (the Company) takes information security and data privacy seriously and carefully. Therefore, the Company maintains the Information Security Management System to ensure business continuity and sustainability, prevent or mitigate potential risks, and maximize the conversion of business opportunities.

The Company develops its information security management system according to the requirements and recommendations of the ISO/IEC 27001 international standard.

This Policy applies to all categories of individuals and entities, regardless of their legal status (employees, individual contractors, subcontractors, sole proprietors etc.), who receive access to Company's systems or equipment, or work on the Company's projects (hereinafter referred to as "personnel").

2. Information security objectives

The Company's objectives of information security supplement are to address information protection and business continuity aspects, in particular:

- Information security and business continuity risks are understood, analysed, monitored, and properly handled.
- The confidentiality, integrity, and availability of the information owned by the Company and transferred by customers to the Company's possession are assured.
- The availability, security, and scalability of corporate systems and services must support the Company's growth and sustainability.

3. Information security principles

At Itransition, the following information security principles serve as the foundation that guides the Company's information security policy:

- The personnel must be aware of and accountable for information security according to the role performed.
- Identified security risks must be continuously monitored. Corrective actions must be taken if unacceptable changes in risk level are observed.
- Information security controls must be provided for Company operational and project development processes.
- Information security incidents must be tracked and communicated among all relevant interested parties.
- Continuous improvement must be encouraged and supported at all levels of the Company hierarchy.

4. Leadership commitment

The Company's executives are fully committed to ensuring compliance with the principles and requirements of ISO/IEC 27001 and the information security regulations of the countries where the Company operates.

5. Continuous improvement

The Company's executives undertake all the required efforts to ensure continuous monitoring and analysis of the information security situation within the Company and constant improvement of the information security.