



<b>Full Name</b>	<i>POL02 SD01 Organizational Information Security Policy_V02</i>
<b>Purpose</b>	<i>To set up scope of the Information Security Management System (ISMS) in DODO Group and declare the commitment of the DODO senior management to comply with the standards set by this Policy</i>
<b>Release date</b>	1.5.2023
<b>Applicable</b>	This internal standard is intended for the internal use of DODO Group SE. The standard is directly applicable to DODO Group SE and is also intended for implementation within the DODO group. The management of the DODO group companies will ensure the implementation of this standard into their internal documentation, which is binding for their employees.
<b>Document location</b>	SharePoint Document Library
<b>Replaces</b>	-

**Content:**

1	INTRODUCTION.....	2
2	GOALS .....	2
3	SCOPE.....	2
4	DOCUMENTATION .....	2
5	POLICY .....	3
6	SECURITY RESPONSIBILITIES .....	3
6.1	BASIC RESPONSIBILITY.....	3
6.2	MANAGEMENT LIABILITY.....	3
6.3	RESPONSIBILITY OF THE INFORMATION SECURITY MANAGER .....	4
6.4	RIGHTS AND PRIVILEGES OF THE INFORMATION SECURITY MANAGER.....	4
6.5	GENERAL RESPONSIBILITY.....	4
7	VALIDITY.....	4

Responsible Director	Approved by	Approved by
<p>T. Fiurášek <i>Chief Technology Officer</i> <i>DoDo Services s.r.o.</i></p>	<p>M. Marek <i>Member of Board of Directors</i> <i>DoDo Group SE</i></p>	<p>M. Menšík <i>Head of Board of Directors</i> <i>DoDo Group SE</i></p>



## 1 Introduction

This document defines “Organizational Information Security Policy” (OIS Policy) of DODO Group.

The OIS Policy applies to all business activities within the scope of the Information Security Management System (ISMS) and covers information, information systems, networks, the physical environment, and the relevant personnel that provides these business activities.

## 2 Goals

- Establishes the organization's policy of protecting the confidentiality, integrity, and availability of its assets, i.e., hardware, software, and information processed by information systems, networks, and applications.
- Identify individual responsibilities connected to information security.
- Provide references for the ISMS security documentation in the above-mentioned scope. To protect the confidentiality of assets against unauthorized disclosure.
- Ensure integrity to protect assets against unauthorized or accidental modification and ensure the integrity and completeness of the assets of the organization.
- Ensure that assets are available whenever necessary in line with the organization's business objectives.
- To ensure that those initiating transactions or interacting with systems can be adequately traced and monitored.
- Ensure work with information in an organizational environment in accordance with applicable Czech law and contractual obligations the organization has towards contractual partners.


## 3 Scope

This policy is valid for all information systems, networks, applications, locations, and employees for all organization processes.

## 4 Documentation

The follow-up security documentation consists of:

- **SD02 Information handling rules** - this is a document that defines the main principles of safe work with information, its transmission, storage, and disposal. This document is binding on all employees of the organization and is reasonably binding on all third-party employees with access to the organization's information assets.
- **SD03 Basic Rules for Computer Use** - this document specifies the principles of computing and information processing. The document is binding on all employees of the organization and is reasonably binding on all third-party employees with access to the organization's information assets.
- **SD04 Rules for Security Incident Response** - The document defines in more detail the rules for reporting, recording and security incident assessment.
- **SD05 The Security Manager** - This document defines in detail the competencies, responsibilities and responsibilities of the security manager role needed to manage information security in the organization.
- **SD06 Guide for Administrators** - this document specifies the principles of computing and information processing. The document is binding on all information system administrators.
- **SD07 Security Software and Tools** – This document details what software and tools is used so that the processes are managed efficiently and with modern approaches.
- **SD08 Security and Technological Documentation** – This document contains technological documentation of the solution with a focus on security.

	Policy 02 IT Security Document 01	<b>Version 2</b>
	<b>Organizational Information Security Policy</b>	<b>Valid from</b> <b>1.5.2023</b>
		<b>Page 3 / 4</b>

## 5 Policy

The Global OIS Policy is expressed as follows:

- Information systems, applications, and organizational networks are always available when needed. They can only be used by legitimate users and contain complete and correct information. Information systems, applications, and networks must also be able to resist damage or recover following threats.

To ensure this, the organization commits itself to:

- Protect all hardware, software, and information assets under its control locally and remotely (i.e., including cloud services and resources). This will be achieved by implementing a system of balanced technical and non-technical measures.
- Perform an efficient and effective protection proportionate to the risks posed to assets.
- Implement the OIS Policy consistently.

Where relevant, the organization will maintain compliance with the legislative standards that apply. The organization will comply with all binding legal standards, as applicable. Information will only be used for the purposes for which it was intended.

The organization will conduct a periodic assessment of security risks (risk analysis) for all business processes covered by this OIS Policy. These risk assessments will cover all information systems, applications, and networks supporting these business processes. The risk assessment will determine the appropriate security countermeasures needed to guard against potential adverse incidents in terms of confidentiality, integrity, and availability of information. Risk assessments will be conducted based on a risk management plan, at least once a year. The Security Manager is responsible for performing the risk assessment.

All users of information systems, applications, and networks are provided with the necessary security advice, enhanced security awareness and, where appropriate, training to increase their security responsibilities.

Irresponsible conduct or misconduct can lead to disciplinary punishment. The organization ensures oversight/responsibility for each project to provide the conditions for the effective implementation of security countermeasures, to create appropriate security documentation, safety guidelines and recovery plans. These requirements are an integral part of each project.

Security incidents must be reported and recorded in accordance with the requirements of the organization's incident reporting system.

## 6 Security responsibilities

### 6.1 Basic Responsibility

The organization's Board of Directors delegates responsibility for the security, policy and implementation of this policy in the context of IT, its development and use in the organization to the Information Security Manager.

### 6.2 Management Liability

Management is responsible for:

- Creating conditions for information security by establishing an overall OIS Policy in an organization.
- Appointment of Information Security Manager and creation of conditions for its work.
- Approval of security exceptions - a written record of each exception must be kept.



### 6.3 Responsibility of the Information Security Manager

The Information Security Manager is responsible for:

- Creating a central site/location for addressing information security issues in the organization in relation to employees and external organizations.
- Implementing an effective way of managing information security.
- Formulating information security policy and supervising its compliance.
- Design organizational standards, procedures, and recommendations in the field of information security.
- Coordination of security activities, especially when sharing information systems and IT infrastructure with external entities.
- Regular information / once a year / management of the organization on the state of information security in the organization,
- Maintaining contact with external organizations and state administration bodies in information security, including representing the organization in relevant institutions.
- Ensuring that IT security risks are acceptable. The level of application of countermeasures established based on the results of the risk analysis.
- Performing Risk analysis as a periodic process which should be repeated a minimum of once per year.
- Ensuring that access to the organization's assets is limited to those who have the necessary permission and authority to do so.

### 6.4 Rights and Privileges of the Information Security Manager

The Information Security Manager is empowered to enforce the OIS Policy, designing, and implementing rules as appropriate.

For example:

- Monitoring and auditing information systems.
- Addressing security incidents.
- Creating access control solutions to information systems.
- Security issues related to purchasing or developing software, hardware, and service delivery.
- Planned and unscheduled audits related to adherence to the organization's security policy.

### 6.5 General Responsibility

All employees of the organization or other entities acting for the organization must:

- Protect the hardware, software and information that is entrusted to them.
- Report any suspected or actual security incidents.
- Report any actual or suspected risks.

## 7 Validity

This policy will be reviewed by the Information Security Manager once a year. Related safety standards are part of the ongoing development and revision program.