# **POLICY ON THE INFORMATION SECURITY SYSTEM**

|  |  |  |  |
| --- | --- | --- | --- |
| **Naziv** | Policy on the Information Security System | | |
| **Datum** | ${psis\_01} | **Verzija** | 1.0 |

Organization - Controller: ${psis \_02\_a}

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of authorized representative

1. Purpose

This Policy on the Information Security System **(“the Policy”)** regulates the measures and procedures used to prevent loss or unauthorized disclosure and regulates the detection and elimination of consequences in the event of loss or unauthorized disclosure of personal data processed by the controller ${psis \_02\_b} (“**Organization**”), as well as official information of the Organization.

1. Definitions

All definitions in this Policy written in capital letter (e.g. Personal Information) shall have the same meaning as those defined in other internal acts of the Organization, unless otherwise expressly specified and defined in this Policy.

The terms referred to in this Policy shall have the following meaning:

**Official data:** document, i.e. any written, reproduced, drawn, pictorial, printed, recorded, photographed, magnetic, optical, electronic or any other record of data, knowledge, measure, procedure, subject, oral communication or information, which, with regard to its content, has the importance of confidentiality and integrity for the Organization, in particular business secrets and Personal data, information on concluded contracts and essential components of the contract, on the terms of provision of services by the Organization, know-how of the Organization, etc.

**Information system:** a computer, communication or other electronic system in which Official Data are processed, stored or transmitted in such a way as to be accessible and usable for authorized persons, comprising the technical infrastructure, organisation, persons and procedures by which the data are processed, stored or transmitted.

**Approach:** any action involving the possibility of consultation, retrieval, disclosure, modification or erasure of data;

**Security Measures:** a set of measures and procedures, at technical and organisational level, the application of which achieves and maintains an acceptable level of security protection of the Information System.

**Security Incident:** an event that threatens the confidentiality, integrity and availability of Official Data, the integrity and security of the Information System, or indicates unauthorized access to the Information System.

1. Application of the Regulation

These Rules bind all employees (Authorized Persons) and external associates of the Organization who are permitted to access the Information System.

External associates of the Organization may, if necessary, be granted the rights of the Authorized Person, provided that the provisions of this Policy shall also apply in respect of them.

Violation of the provisions of this Policy by the authorized persons may lead to the extraordinary termination of the employment contract, and in case of violation by external associates of the Organization, the termination of the contractual relationship.

1. Rights and obligations of authorized persons

Authorized Persons shall be appointed by the responsible person within the Organization, and Authorized Persons shall be determined regarding the workplace and in accordance with the business processes they carry out, and in this connection the scope of authorization to access the Information System shall be determined in accordance with the needs of their workplace.

The scope of the authorization to access the Information System granted to the authorized person shall not exceed the powers vested in the Authorized Person in the regular business process.

Authorized Persons shall comply with the provisions of this Policy in order to ensure proper operation and security of the Information System and to prevent security incidents.

Authorized Persons are obliged to take all the Security Measures prescribed in this Policy as well as other reasonable security measures to ensure proper operation and protect the security of the Information System and prevent or eliminate Security incidents.

1. Protection of the Information System

**5.1. Control and protection of access**

The responsible person within the Organization grants rights for access to the Information System to authorized persons in accordance with the needs of their workplace, to the minimum extent necessary for the performance of work tasks within the framework of the regular business process.

The responsible person within the Organization shall keep records of access approvals and shall review the same records and powers as a result of any significant change to the system and at least once a year.

Authorized Persons when accessing the Information System are identified by using the username and password, and Authorized Persons are responsible for the selection and preservation of the confidentiality of the passwords they use.

When choosing a password, the Authorized Person must take care to use a strong and regularly modified password (at least once a year), which shall contain at least 12 characters and shall contain one or more of the following: capital letters (ABCDE...), lowercase (ABCDE...), figures (0-9), symbols (@#$%{}/\'”; . & & >...), punctuation characters (?!).

The Authorized Person is obliged to keep the password secret and not disclose it to other persons. Exceptionally, if there is a justified need for access to a particular part of the Information System by another Authorized Person, and that part can be accessed exclusively through the Authorized Person’s password, the Authorized Person may disclose the password to another Authorized Person. In such a case, the Authorized Person who has given the password is obliged to replace the password without delay as soon as possible.

In the event of force majeure or absence from work, the authorized person, with the advice, if applicable, of the person responsible for the protection of personal data in the Organization, who is the system administrator, may inspect the Organization’s Information System for the purpose of insight of Official Data. Such insight is carried out only in relation to Official Data and data necessary for inspection (e.g. agreement with a business associate on products and services, agreed prices and dates) and after inspection a log of access is made.

**5.2. Rules of use of equipment**

The equipment of the Organization may be used exclusively for business purposes, and all equipment must be recorded and recorded by all users of the equipment.

The equipment of the Organization shall not be used for private purposes except with the express permission of the Organization.

The use of the Organization’s equipment, i.e. personal equipment used for business purposes, must be in accordance with the law, internal acts of the Organization and license rights.

The equipment of the Organization must be adequately protected (antivirus protection), appropriate to the particular type of equipment of the Organization.

Authorized Persons are responsible for the professional, ethical and lawful use of the Organization’s equipment and personal equipment when used for business purposes.

The equipment of the Organization, i.e. personal equipment when used for business purposes, must, where technically possible and do not require disproportionate effort, be protected by an appropriate complex password or by any other means which prevents direct access to it by third parties other than the Authorized Persons.

Authorized Persons are obliged to change passwords for access to the Organization’s equipment, i.e. personal equipment used for business purposes, at least once a year.

Authorized Persons are obliged to take all necessary security measures to prevent the alienation of corporate equipment, i.e. personal equipment used for business purposes.

Authorized Persons shall not place the equipment of the Organization for use by third parties, and in the case of supply of personal equipment used for business purposes, they shall take all reasonable security measures to prevent the occurrence of a Security Incident.

## **5.3. Rules of use of personal equipment**

The use of personal equipment for business purposes poses a risk to the business, to the greatest extent present as a risk of unauthorized access, theft and loss of data.

It is permitted to connect its own data storage devices (e.g. external disks) to the Organization’s equipment for the purpose of backing up the data and transmitting the data in case this is not possible or is not sufficiently practical to work through the Information System. Before using your own data storage device, it is necessary to check the device and its content with an antivirus tool. It is not permitted to connect and use devices infected with viruses or other malicious programs. If the data storage device is outside the premises of the Organization, the official and personal data on the device must be encrypted and additionally protected by a password to access the device, if the device has this possibility. When all data is no longer needed, it must be deleted in a secure manner.

It is not permitted to copy and store internal and confidential data on its own devices without prior approval by the Organization. It is not permitted to copy and store data marked as a trade secret on its own devices and storage media, even in encrypted form.

## **5.4. Use of official information systems and e-mails**

Authorized Persons shall use official Information Systems of the Organization and official e-mails of the Organization in such a way as to avoid harm to the Organization and the occurrence of a Security Incident.

Content sent by official e-mail must be written carefully and measured in order to avoid a Security Incident.

The e-mail service may only be used for official communication. It is prohibited to send e-mails from the official e-mail address for private purposes.

Messages on the official e-mail service are considered official documents.

It is not permitted to automatically forward emails to another user account, i.e. any other email address not belonging to the Organization, without the permission of the Administration of the Organization.

Upon termination of the employment or other contractual relationship, the Authorized Person of IT Support of the Organization must ensure that the user account of the Authorized Person is closed, in such a way that the user account is deactivated with the last day and sends an automatic electronic message to the senders to whom they can contact, and then after 2 months the user accounts are deleted.

## **5.5. Internet access and use of internet services**

 The Internet can be used exclusively for business purposes, information and education.

The Organization shall take appropriate security measures to prevent unauthorized online access to the Organization’s Information System, and in particular protective measures against viruses and other destructive programs, including the installation and running of programs to protect against viruses on equipment (devices) used for internet access.

Programmes used to protect against viruses shall be kept up to date and authorized persons shall not exclude or disable such updates and programmes.

Authorized persons are obliged to avoid online activities that could compromise the security of their computers and the Information System of the Organization, and when using the Internet, they may visit only pages that are necessary for the performance of the work.

**5.6. Additional protection measures**

In order to protect the Information System, the Organization shall also implement the following protection measures:

* Protection measures to prevent unauthorized persons from using the Information System:

${psis\_03}

* + ${psis\_03\_item}

${/psis\_03}

* Measures to ensure that the data contained in the Information System cannot be read, copied, changed or removed without appropriate authorization during the process of electronic transfer, transport or storage on data media, and that there is a possibility of checking and identifying the recipient to whom personal data is to be transferred through data processing systems:

${psis\_04}

* + ${psis\_04\_item}

${/psis\_04}

* Measures to ensure that the data contained in the Information System are protected against accidental destruction or loss:

${psis\_05}

* + ${psis\_05\_item}

${/psis\_05}

1. Notification of a Security Incident

Authorized Persons and external contractors authorized by the Authorized Persons shall, without delay, inform the management of the Organization or an authorized person designated by the management of the Organization if they become aware of any security incident and of any violation of the provisions of this Policy, or if they detect any deficiencies in the functioning of the Information System, and in particular in the security measures of the Information System.

1. Final provisions

Upon termination of the employment contract or contractual relationship with the Organization, all Authorized Persons shall be obliged to return the equipment of the Organization, as well as any other property assigned to them for use. Also, all Authorized Persons are obliged to submit all documentation and all information owned by the Organization. It is not permitted to copy and disclose the Official and Personal Data entrusted to the Authorized Persons.

This Policy shall enter into force eight days after the date of their publication.

This Policy shall be appropriately disclosed to the Authorized Persons, and the period of adaptation for the full application of this Policy shall be one month from the date of adoption.