OIV Digitalni signali i mreže

ISMS-ZAP-009
INFORMATION SECURITY REQUIREMENTS FOR SUPPLIERS, VENDORS AND BUSINESS PARTNERS

Version:	1.0
Confidentiality level:	OIV_PUBLIC
Publication date:	25 May 2022

List of abbreviations / definitions	Description
Supplier / Vendor	Any natural or legal person with a legal capacity to enter into a contractual relationship with the Company for the purpose of: • procuring goods, materials, energy and other resources necessary for information systems maintenance and functioning; • external service provision for information systems development and maintenance including execution of works
Company	Odašiljači i veze d.o.o.
Availability	A feature which ensures that information resources are available to authorized persons when needed.
HTTPS	*HyperText Transfer Protocol Secure* is an Internet protocol created by combining HTTP with SSL / TLS
Information	Information is processed, organized and structured data. It provides context for data and enables decision making processes.
Information system	Any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.
Information security incident	Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
Integrity	A requirement meant to ensure that information can be changed only in a specified and authorized manner.
IT	Organizational unit responsible for core networks, IT and services.

IT device	A piece of physical hardware that is used to compute or support computer functions within a larger system.
User	Any person who uses company information systems for business purposes under applicable contracts.
Information owner	Head of the organizational unit with operational authority for specified information within information system.
Confidentiality	The property that data or information is not made available or disclosed to unauthorized persons or processes.
SFTP	*Secure File Transfer Protocol*
SSH	*Secure Shell Protocol*
Business partner	A person who is not an employee of the Company and concludes contracts of any kind other than purchase and sales contracts (e.g., temporary service contract or copyright contract).

Content

1. Purpose

All vendors and business partners must be aware that even unintentional or accidental breaches or a minor negligence can lead to an information security incident. Information security incidents may have far-reaching repercussions such as legal implications relating to Company's compliance with regulatory requirements (e.g. legal proceedings for non-compliance with regulatory requirements), performance of tasks (e.g. inability to perform contractual obligations due to unavailability of business-critical systems), reputational risk (e.g. hackers attempt to release confidential information could create reputational risks and negative media coverage), financial impact and negative cash flows (e.g. data breach fines and penalties, loss of revenues due to unavailability of business-critical systems).

2. Scope

Information security requirements for suppliers, vendors and business partners provide security guidelines for all suppliers, vendors and business partners who enter into a contractual relationship with the Company and exchange confidential or personal information. By understanding, accepting and committing to comply with these security standards and requirements, suppliers, vendors and business partners will be able to appropriately manage data and information, computer equipment and information systems in a secure and safe manner.

These information security requirements apply to all suppliers, vendors and business partners of the Company. While managing Company's data, computer equipment and/or information systems, suppliers, vendors and business partners shall commit to comply with information security requirements.

These security requirements refer to Company's data and information, as well as all supporting information systems that suppliers, vendors and business partners may have access to during data processing.

This document specifies minimum mandatory security requirements for suppliers, vendors and business partners of the Company in accordance with the Information Security Policy.

3. Information security requirements for suppliers, vendors and business partners

3.1. General requirements

All information, computer equipment (e.g. laptops, desktops, smartphones, USB, CD / DVD) must be treated with the care, attention and diligence. Information and data shall not to be forwarded to private e-mail addresses, stored, sent to public cloud services or other platforms not approved by the Company or otherwise stipulated in the contract. Suppliers, vendors and business partners shall refrain from any activities that may adversely affect the Company's information systems, including the following activities (but not limited to):

- access, download or distribution of: illegal content, violent content, discriminatory content, pornographic content, advertising content, chain e-mails, suspicious and malicious e-mails

containing unknown links or suspicious attachments, or phishing emails mimicking manager's instructions for fund transferring
- violation of laws and other regulations, infringement of intellectual property rights or violation of licensing agreements
- gambling and mining cryptocurrencies (e.g. Bitcoin, Ethereum)
- activities that may result in denial of service or business interruption
- bypassing security controls

Suppliers, vendors and business partners shall restrict the use of insecure communication protocols, and shall use secure and up-to-date communication protocols (e.g. SSH, HTTPS, SFTP) when communication takes place via public networks, including the Internet.

All security incidents and related alerts reported by organizational unit in charge of IT security shall be taken seriously and suppliers,vendors and business partners shall act in accordance with the procedure following receipt of the notification.

3.2. Mandatory use of user accounts

Each supplier, vendor and business partner with access to the Company's information systems shall be assigned a user account. All suppliers, vendors and business partners shall protect their user accounts in order to prevent misuse.

This includes (but is not limited to) the following:

- the supplier or business partner shall not share their user accounts
- in case of suspicion that user accounts have been compromised, it is necessary to immediately inform the contact person of the Company or use any of the agreed communication channels

3.3. Choice and use of passwords

All suppliers, vendors and business partners shall ensure the use of strong passwords. The proposed minimum requirements for strong password are following:

- minimum length of 8 characters
- at least one uppercase letter, one lowercase letter, one number and one special character
- the use of personal data (e.g. name, birthday, employee identification number) is prohibited
- the use of keyboard patterns (asdf) or sequential numbers (1234) including dictionary words are not recommended

Passwords must be kept secret. In case of suspicion that password has been compromised, it is necessary to immediately inform the contact person of the Company or use any of the agreed communication channels.

The use of *passphrase* is allowed, provided that the rules defined for passwords are conformed to, and passphrases must contain at least 15 characters.

3.4. Information classification

All suppliers, vendors and business partners shall ensure appropriate information and data management in the manner described below.

Confidentiality level	**PUBLIC**
Physical and administrative control	None
Duplication	Unlimited
Storage	No restrictions
Distribution	No restrictions
Destruction/disposal	Recycling/waste
Approval for disclosure to third parties:	Not necessary

Confidentiality level	**INTERNAL**
Physical and administrative control	• **Information owner:** accountable for proper labelling of all data • **User:** responsible for the proper storage, processing, distribution, duplication, destruction and document control
Duplication	Only employees, suppliers, vendors and business partners with duly signed confidentiality agreements may duplicate to a limited extent
Storage	• **In paper form:** to be kept under lock when not in use • **In electronic form:** only on those resources which are made available or are approved by IT
Distribution	• **Internally:** an envelope is to be used to deliver mail internally • **Externally:** a sealed envelope must be used • **In electronic form:** When sending an email internally or externally, special attention should be paid when entering the email address of the recipient • **By fax:** check the fax number
Destruction/disposal	• **Paper documents**: documents must be shredded and disposed of in a paper container • **Electronic data:** delete the data
Approval for disclosure to third parties:	Information owner

Confidentiality level	**CONFIDENTIAL**
Physical and administrative control	• **Information owner:** responsible for proper labelling of all data • **User:** responsible for the proper storage, processing, distribution, duplication, destruction and document control
Duplication	Only employees, suppliers, vendors and business partners with duly signed confidentiality agreements may duplicate to a limited extent
Storage	• **In paper form:** to be kept under lock when not used • **In electronic form:** only on password-protected resources approved by IT
Distribution	• **Internally:** an envelope is to be used to deliver mail internally • **Externally:** a sealed envelope must be used Mail can be delivered in person or sent by registered mail using courier services and similar • **Electronic distribution- internally:** Email encryption in internal email communications is recommended In that case, a password must be provided through another communication channel • **Electronic distribution- externally:** Email encryption in external email communications is required In that case, a password must be provided through another communication channel • **By fax:** check the fax number
Destruction/disposal	• **Paper documents:** to be shredded or disposed of in secure document destruction containers • **Electronic data:** data must be erased, contact IT for support
Approval for disclosure to third parties:	Information owner

Confidentiality level	**SECRET**
Physical and administrative control	• **Information owner:** is responsible for proper labelling and must ensure that strictly confidential information is disclosed in accordance with the need-to-know principle • **User:** is responsible for encryption of strictly confidential information and/or must ensure that strictly confidential information is kept under lock when not used
Duplication	It is possible to make a limited number of copies if the information owner, or person designated by him, is present.
Storage	• **In paper form:** to be kept under lock when not in use

	• **In electronic form:** only on password-protected resources approved by IT
Distribution	• **Internally:** a sealed envelope must be used Delivery should preferably be made in person • **Externally:** a sealed envelope must be used Mail can be delivered in person or sent by registered mail using courier services and similar • **In electronic form:** Email encryption in internal and external email communications is required In that case, a password must be provided through another communication channel • **Sending a fax:** right before the information is faxed, it is necessary to get a confirmation via telephone that a test page has been received. It is also necessary to get a telephone confirmation that all documents have been received
Destruction/disposal	• **Paper documents:** they must be shredded in a document shredding machine • **Electronic data:** they must be erased. Contact IT for support.
Approval for disclosure to third parties:	Management of the Company

All information that is not explicitly classified and all information containing personal data must be deemed as information classified as "Confidential".

Information with the level of confidentiality classified as "Internal", "Confidential" and "Secret" is considered a trade secret.

3.5. Clean desk/screen policy

- When leaving their desk, employees must lock their computer screens, that is, log off and lock their smartphones. Screens mus be set to lock automatically after a maximum of 10 minutes of inactivity.
- At the end of a working day, an employee must log out or lock the devices.
- Information classified as "Internal", "Confidential" and "Secret" must not be left on the desk if the user is not present. Information must be placed in a locked drawer or cabinets.
- passwords, PINs or other personalized information must not be written down and left in plain view.
- it is necessary to ensure that printed information classified as "Internal", "Confidential" and "Secret" is not left in printing devices,
- writing boards or other media for visual presentation which contain information classified as "Internal", "Confidential" and "Secret" must be cleared after use.
- Information, especially documents and equipment used in meetings, must be removed once the meeting is finished. Information that users no longer need will be destroyed.

3.6. IT devices processing information of the Company

- IT devices will be equipped with an operating system which is updated according to manufacturer's instructions
- antivirus solutions must be installed on user devices
- an IT device must be protected with access controls
- an IT device must be protected from unauthorized use
- IT device will not be given to unauthorized persons (including family members)
- logs must be kept of information system use in order to ensure responsibility and non-repudiation
- security logs will be protected from unauthorized modification or deletion

3.7. The use of the Company's information assets for private purposes

- all information, assets or services owned by the Company will be used solely for business purposes
- Storage of private data on the Company's resources is prohibited. The Company can delete all private information stored on the resources of the Company without a prior notice to the user.
- Suppliers, vendors and business partners are aware of the fact that all their activities on the Company's information systems can retroactively be detected and investigated in case of any suspected misconduct

3.8. Storage of business information

- Suppliers, vendors and business partners can store the Company's information on their own IT equipment in accordance with the guidelines specified in this document
- business information may not be stored on public cloud computing services which are not approved by competent organisational units of the supplier, vendor or business partner
- all information must be stored securely and protected from unauthorized access depending on the information classification

3.9. Disclosure of information and use of equipment

- information and IT devices may not be copied or taken out of office without the express permission of the information owner
- suppliers, vendors and business partners must ensure all necessary measures in public places to prevent the disclosure of confidential information

3.10. Communication

- Suppliers, vendors and business partners must employ due care to protect communication from unauthorized access or eavesdropping
- Suppliers, vendors and business partners must use VPN communication to access the infrastructure of the Company
- only secure communication protocols will be used to transmit information in line with the classification of information.

3.11. Reporting on information security incidents

- Suppliers, vendors and business partners will notify the Company of any security incidents by contacting the responsible person in the Company or directly to the email address noc@oiv.hr or by phone at +385 1 6186 666 or +385 1 6186 667
- Suppliers, vendors and business partners will provide necessary support to analyse and resolve the incident.