

Pursuant to Article 39 of the Statute of ALICORN doo Podgorica (hereinafter: the Employer), the founders, on 15th of October 2021, adopt the following:

Information Security Policy

ALICORN doo Podgorica

1. Ownership of information

Each information resource (data, information, metadata, procedures, software and hardware for processing of information, human relations, services), whether in paper or electronic form, has one and exactly one owner who is responsible for taking care of it in terms of information security. This ownership does not imply ownership in a legal sense.

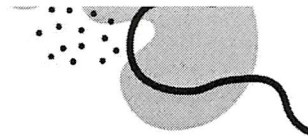
The owner is obliged to categorize the information in terms of value, confidentiality and legal requirements. The potential need for the availability and sharing of this information shall be taken into account whilst the information is being categorized.

2. Portable media

The employee is obliged to keep a register of portable media (phones, laptops, computers, tablets, memory cards, USB...) that he or she manages, in order to reduce the risk of data loss. All removable media shall be stored in a safe place, in accordance with the manufacturer's specifications.

When the media is not in use, it shall be disposed of safely, in a locked container (drawer, cabinet, safe...) and protected from unauthorized access. When the media is no longer in use, it shall be destroyed or deleted in a way that data recovery is not possible.

Passwords shall be secure, changed regularly in accordance with industry standards, and under the responsibility of the owner of the password as a resource.



Password sharing shall be kept to a minimum. The owner of the password, which is considered a resource, is responsible for its sharing. When terminating an employment relationship with someone who has had access to passwords or when changing their responsibilities, the password shall be changed.

Medium used for business purposes should not be used for private purposes.

3. Confidential information

All confidential information (information on the business of the Employer, the client and related persons and organizations, the trademark and seal of the Employer, contracts, other information that has the character of confidentiality...), regardless of the media on which they are located, shall be protected from unauthorized access.

Access to confidential information by third parties shall be kept to a minimum, and done in the presence and constant supervision of the owner of the information.

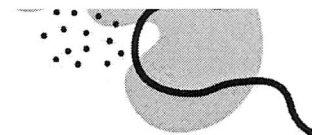
All information, no matter what medium it is on, shall be secured and protected physically as well.

Any access to confidential information by a non-owner of that information as a resource shall be recorded.

Unauthorized disclosure of confidential information is prohibited.

Outside working hours, there shall be no confidential information on the employee's desk, regardless of the medium on which it is located.

The exchange of electronic information (messages, transactions) shall be protected in proportion to the sensitivity of the information.



The employee is obliged to respect the rule of "clean table" in the sense that when the employee is not at work, all documentation and information shall be stored in a safe place. Also, the employee is obliged to respect the rule of "clean screen", i.e. that information that is considered confidential cannot be displayed on the computer desktop.

The Employer is obliged to keep and process personal data related to the employee in an adequate manner and with special care.

The Employer is obliged to acquaint the employee with what personal data he processes as well as with the rights that the employee has in relation to his personal data (right of access, right to correction, right to deletion...)

4. Information Backup

In the backup of information, redundant mediums should be used and alternated regularly to minimize the consequences of loss of medium function.

The owner of the information takes care of the need for backup of information and its frequency.

The frequency and manner of backups should reflect the business and security requirements of the information, as well as how crucial it is to ensure business continuity.

Mediums containing backed-up information shall be equally or better protected than those containing original information. Mediums that have backup copies shall be tested regularly, to make sure that they can be counted on in case of emergency.

Information recovery procedures shall be tested regularly.

5. Procedures in case of termination of employment (employment or contractual relationship)



The obligation to take care of information security is part of the employee's work obligations and is valid for the entire duration of the employment contract or a contract on specific work to be done. In special and clearly communicated cases, this obligation may continue to apply after termination of employment or contractual relationship.

The owner of the resource takes care of access rights to the resource. Resource access rights for an employee or third party shall be terminated immediately upon their termination of employment or the confidentiality agreement.

After the termination of employment, employees are obliged to return all property to the Employer.

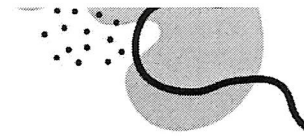
In the event that the employee uses his property for work processes, the employee is obliged to ensure that the information related to the Employer is destroyed or deleted upon termination of employment so that their return is impossible.

In case of termination of employment, the employee is obliged to delegate all assets and return all mediums received from the Employer for use for work. In case the employee keeps a medium, which he received from the Employer, after the end of the employment he or she is obliged to transfer all information before leaving the job and destroy and/or delete information related to his work with the Employer while the Employer is obliged to perform a check.

The employee is obliged to transfer access to emails and other accounts, and the Employer is obliged to change the access parameters on the online platforms and services to which the employee had access.

Changes in ownership and responsibilities are treated as the cessation of existing ones and the beginning of new ones.

6. Confidentiality Agreement



Granting access to sensitive information to a third party shall be preceded by the signing of a confidentiality agreement. It defines:

- Information to be protected,
- Period of validity of the agreement,
- Responsibilities of the parties,
- The right to be checked and monitored by the Employer for activities involving confidential information.
- Notification process in case of unauthorized access to information,
- Conditions for return and destruction of information after the expiration of the agreement in accordance with other normative documents of the Employer,
- Activities to be taken in case of breach of agreement.

The signatories of the confidentiality agreement are obliged to respect its provisions for the period for which the agreement was concluded as well as within three (3) years after the end of the period for which it was signed.

In addition to the confidentiality agreement, the employee is obliged to comply without exception with the confidentiality clause contained in the employment contract or in the contract on specific work to be done. The employee is obliged to respect the confidentiality clause even after the end of the employment or contractual relationship, for three (3) years after the end of the employment or contractual relationship.

7. Change to the data or data processing and data display systems

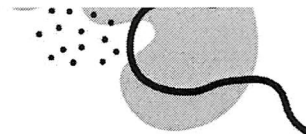
Any change to the data or data processing and data display systems shall occur in accordance with the following:



- The change shall be identified and documented before its application.
- The change shall be proposed by an authorized person.
- The change shall be approved by the owner of all resources affected by the change. The approval shall be in written form, unless otherwise specified in another document.
- The change shall be planned and tested.
- Owners of all resources and stakeholders affected by the change shall be informed about the beginning, the process itself and the completion of the change. This information shall be written, unless otherwise specified in another document.
- The change is to be made at a convenient time so that it does not interfere with other work processes.
- The way in which change affects other established processes and resources shall be documented and communicated to stakeholders.

Before installation of a new information system, and/or of certain changes, and/or of certain components the following shall be considered:

- System performance and required capacity.
- Procedures for system recovery in the event of an error.
- Continuity plans.
- Preparation and testing of operational procedures.
- Establishment of security controls.
- Evidence that the installation will not adversely affect existing systems.



- The impact that the installation of the system or of the change has on the overall performance and security.
- Necessary training.
- Ease of use.

8. Proceedings in the event of a breach of the security, availability or integrity of information or resources

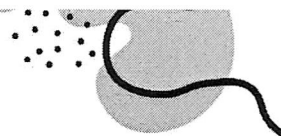
In the event of an incident related to the safety, availability, or integrity of the resource, the employee shall not take any action in terms of recovery before notifying and obtaining the written consent of the resource owner.

Incidents shall be adequately documented.

When the response to a security incident involves the initiation of legal proceedings, the evidence shall be collected, stored and presented adequately and in accordance with legal regulations. The integrity of the evidence shall be protected and all actions shall be performed only on copies. Copying of evidence shall be supervised by authorized persons and all copying information shall be documented in detail.

The information security management system is based on the PDCA model (plan-do-check-adjust) which has the concept of continuous improvement at its core.

Non-compliance with the Safety Policy is considered an offence that the employee commits and may be subject to disciplinary, material and criminal liability.



ALICORN DOO PODGORICA

Founders

Sauja Gorksen

