Protocol No: 4853 / 14 Tirana, on 06/08/2021

C2 Internal

| **I-PURPOSE** |
|---|
| The purpose of this policy is to define the rules on how to classify, handle and store a certain information or document by OST sh.a. employee during the exercise of his/her duties and functions. Information must be appropriately protected in accordance with the risk level it presents and the information classification aims to mitigate such risk. |
| **II - SCOPE AND COMPATIBILITY** |
| This policy shall apply to all OST sh.a. staff. Implementation and compliance shall be monitored on a regular basis and the results shall be reviewed by the relevant OST sh.a. sectors in cooperation with the Directorate of Corporate Affairs. Any violation of such procedure shall be treated as a disciplinary violation in accordance with the labor code and the relevant OST sh.a. internal regulations. |
| **III- FOR THE ATTENTION OF:** |
| OST sh.a. staff |
| **IV-REFERENCES** |
| This policy makes reference to section A.8.2 of the ISO 27001:2013 Information Security Management System. |
| **V- CONTACT PERSONS** |
| Gerald Bici - Head of Sector, Information Security Policy Sector<br>Majlinda Dhespoti - Director, Directorate for Corporate Affairs |
| **VI- HISTORY** |
| 0.0 - Initial version<br>0.1 - Code change in compliance with the ISO 27001:2013 standard requirements |

| DRAFTED | REVIEWED | ACCEPTED BY | APPROVED BY: | VERSION | DATE | PAGE: |
|---|---|---|---|---|---|---|
| **Gerald Bici**<br><br>Head of Information Security Policy Sector<br><br>(Signature) | **Majlinda Dhespoti**<br><br>Directorate of Corporate Affairs<br>(Signature)<br><br>**Brunilda Veizi**<br>Head of Sector, Legal Directorate\ Administrative and Judicial Affairs Sector<br>(Signature) | **Majlinda Despoti**<br><br>Directorate of Corporate Affairs<br>(Signature)<br><br>**Ilda Neziri**<br>Legal Department and Corporate Affairs<br>(Signature) | **Skerdi Drenova**<br><br>OST sh.a. Administrator<br>(Signature) | Version 0.0<br>Version 0.1 | Date: 17/09/2020<br>Date: 22/03/2021 | 1/ 14 |

## 1. Introduction

The information that is kept, handled or created by any OST sh.a. employee during the exercise of his/her functions is subject to a certain level of confidentiality. Such information must be appropriately protected in compliance with the risk level it presents. The information classification purpose is to determine such risk level.
Pursuant to the ENTSO-E directive for Information Classification and the legislation in force, OST sh.a. has put in place a number of measures to manage such risks related to the release of unauthorized information, as a function of the confidentiality level related to each information.
Beyond the responsibility for confidentiality, which is mandatory for all employees in all circumstances, such classification also enables us to reduce risk and enables safeguards to be defined in order to:
- Ensure the confidentiality of the processed information;
- Limit the fraud risk, confidential information disclosure, information deletion or theft.

## 2. Acronyms

- OST - Transmission System Operator
- AKCESK - National Authority for Electronic Certification and Cyber Security
- ERE - Energy Regulatory Entity
- ENTSO-E - European Network of Transmission System Operators for Electricity
- PDA - Personal Digital Assistant
- USB - Small data storage device
- CD - ROM - Compact disc
- DVD - Data storage device in digital format

## 3. General principles

Any OST sh.a. employee bears responsibility regarding the maintenance or processing of the information it possesses for the fulfillment of his/her work activities as well as whether such information does constitute a business secret, etc.
Compliance with the full implementation of information confidentiality is not just a condition that enables risk protection; it also provides a professionalism guarantee and protection of the reputation of the company and its employees.

Some of the necessary rules are as follows:

### 3.1 Information or documents received

OST sh.a. employees are required to comply with the practical rules for the creation, circulation, storage and destruction of information or documents they receive both during and after their projects. If any employee mistakenly receives information or a document not intended for him/her or that he/she does not need to be aware of, it is his/her responsibility to send this information or document to the sender or drafter of the document and, at the same time, to destroy his/her copy.

### 3.2 Persons who should be aware of the information/document

In accordance with the confidentiality rules, any information or document, regardless of its nature, must be distributed only to persons who should be aware of the information / document, in the context of their function or mission.
In addition to the default information recipients, those who are entitled to know are persons who need to have the information for the exercise of their function or mission, even if they are not officially identified as recipients.
This category includes the assistants of certain recipients if they are delegated by their superior and/or the information owner. Recipient managers must also be aware of any information intended for the recipient unless otherwise specified by the information owner. Auditors also have this right.

### 3.3 Telephone and email conversations

Confidentiality rules must be respected at all times:
- Within the Company: in the central apparatus and in the Operative Units of OST sh.a., etc.
- Outside the Company: in transport, hotels, family facilities, in public places, in restaurants, elevators, halls, etc.;
- In all communication means such as email, social media, newspapers, magazines, television, radio, which are open to a wide audience.

### 3.4 Communication with the media, other institutions

The OST employee is not authorized to speak on behalf of OST sh.a., without prior approval from the Administrator or the Directorate of Corporate Affairs or the managers to whom the authority has been delegated, in case of frequent contact.
In this context, the OST sh.a. employee is not authorized to respond to the requests from journalists or other individuals requesting confidential information without obtaining appropriate approval on the information to be communicated, even if he/she believes that the information is harmless and non-confidential.

### 3.5 Request for information

Based on the instructions of ERE, AKCESK and ENTSO-E, "On the classified information", OST sh.a. is obliged to maintain confidentiality over classified information.
Keeping information confidential means to stop handling information:
- For personal purposes by authorized persons;
- For the purposes of benefits from third parties outside OST sh.a..

### 3.6 Work desk

It is important that the work desk is clean and there are no documents on it. At the end of the work, confidential files and documents must be removed and kept in locked drawers or cabinets. Laptops, cell phones, PDAs, removable drives (e.g., USB keys, etc.) should be locked.
No sensitive documents should be left on printers, photocopiers or fax machines.

During the day, in case of prolonged absence, measures shall also be taken to clear the desk of sensitive documents. Before leaving the meeting room, the person responsible for the meeting must ensure that no sensitive information or documents are left behind.

### 3.7 Rights to enter the office

Any OST sh.a. employee must act in accordance with the rules and systems that control access to the building. According to the OST sh.a. approved regulation "Administration Rule of the Building", unrecognized individuals must not roam freely in the halls beyond the reception area. Such individuals should be handled, asked what they are looking for, and, depending on the situation, they must be escorted or brought to the waiting area. The same attitude should be adopted with regards to customers, visitors and suppliers, even acquaintances.

### 3.8 Relations with contractors

Where information is circulated outside OST sh.a., it is appropriate to provide, where possible also by contract, an appropriate level of protection to handle such information so as to ensure a protection level comparable to that within OST sh.a., pursuant to this instruction. Therefore, the service requester must carefully specify the protection needs of the information which is classified or handled by the service provider. Special attention should be paid to the contract drafting, when the services are performed in the OST sh.a. premises.

In general, precise specifications should be included in the service provider's contract regarding the conditions for the transfer, processing and storage of confidential information.

The paragraphs to be included in the contract provide:

- Obligation of the service provider to guarantee the confidentiality of data that may be communicated to him/her or of which he/she may have knowledge;
- Definition of data that should be considered confidential;
- Duration of this obligation.

Furthermore, beyond the issue of information confidentiality, it is important to define contractual requirements for information security. The purpose of such obligations is to ensure that confidential information is protected by the service provider using the technical, logical and organizational means necessary to avoid any involuntary loss of confidentiality.

This security obligation must take into account the various aspects of the information life cycle:

- Control of access to information, reserving it only for authorized persons;
- Implementation of security measures to ensure the confidentiality and integrity of data, especially for data transfer and/or storage (use of encryption);
- Implementation of measures to avoid the data destruction, whether accidental or not;
- Inclusion of specific measures designed to avoid infections affecting any OST data or information system by malware (viruses, logic bombs, Trojan horses, etc.);

## 4. Principles of information classification and confidentiality protection

The information classification regarding confidentiality and its protection is based on five basic principles.

### Principle 1 - Possession of information

Any information handled within the company is associated with an owner and a holder.
a. Each OST employee is the possessor of the information they generate, unless otherwise stated. When an employee is no longer able to take on the responsibilities associated with ownership (due to a change of Department, dismissal from the company, etc.), the default owner is the superior of the original owner. In case of reorganization, the unit that takes over an activity inherits the possession of the information related to that activity.
In addition to the confidentiality obligation, each holder of information is responsible for assigning an appropriate classification level for confidentiality.
b. The holder is a user who receives information and thus assumes the same rights and responsibilities as the possessor.

### Principle 2 - Classification of information by level

The classification criteria defined for OST sh.a. are as follows:
- **Availability** - being available and usable upon request by an authorized person or entity, within a certain period of time;
- **Integrity** - ensuring that the information, or a procedure for its processing, has not modified or destroyed the information accidentally or without due authorization;
- **Confidentiality** - information may not be disclosed or made available to persons, entities or processes that do not need to know this information or are not authorized;
- **Fact** - being able to prove that an action or event related to the information occurred. It is characterized by the traceability of various actions related to the processing and use of such information (e.g., through the existence and archiving of audit missions).

### Principle 3 - Proportionality and scale of protective measures

The principle of proportionality and scaling of protective measures consists in the protection of each piece of information and/or each system, as a function of its level of confidentiality classification.

### Principle 4 - Information marking

All means of communication containing information, except information that is generally addressed to the public, must be marked appropriately adapted to the context to ensure its readability. This marking associates the information with an appropriate level of protection (e.g., through a standard title inserted into each document, with a certain number of items to be filled in: such as the document classification level, author, reference number, etc.).

### Principle 5 - Continuous review of information classification level

Confidentiality classification is reviewed as often as required by its possessor (or holder). The review process may result in a lower or higher classification level.

## 5. Confidentiality rules for classifying information

### Classification level definitions

### Rule 1 - C4 RESTRICTED

Any information whose disclosure would cause serious damage to OST sh.a vital interests is classified as C4-RESTRICTED.
The highest classification level is the RESTRICTED level. This level refers to information that is highly sensitive and would cause serious reputational damage and financial loss if such information was lost or disseminated incorrectly.
The criteria for assessing whether information will be classified as RESTRICTED include cases where its unauthorized disclosure would:

- materially damage relations with third parties
- prejudice individual safety or liberty;
- cause damage to the operational effectiveness or company security;
- significantly damage the company's financial stability;
- hinders the investigation or would facilitate the commission of a serious crime;
- seriously hinder the development or operation of organizational policies; close or disrupt important OST sh.a. operations
- damage OST sh.a. image causing irreparable damage.

Access to information assets designated as "RESTRICTED" shall be strictly controlled by senior management and in many cases numbered copies of documents will be distributed according to specific procedures.
In practice, the number of items of information classified C4 RESTRICTED is extremely limited.

### Rule 2 - C3 CONFIDENTIAL

Any information to be communicated only to persons directly concerned (and specifically identified) and the unwanted disclosure of which could damage a project, activity or unit of OST sh.a., is classified as C3 CONFIDENTIAL.

The most protected level is the confidential one.
The criteria to assess whether information will be classified as confidential include cases where its unauthorized release would:

- negatively affect relations with other organizations
- cause great distress to individuals
- cause potential financial loss or loss of profit or facilitate unfair advantage or advantage to individuals or companies
- prejudice the investigation or facilitate crime commission
- violate the appropriate commitment to maintain confidentiality of information provided by third parties
- hinder the development or effective implementation of organizational policies
- violate legal restrictions on information flow
- disadvantage OST sh.a. in commercial negotiations or policies with third parties
- harm the proper management of the organization and its operations

Information falling under "Confidential" classification shall usually be handled by middle management and above, with some lower hierarchical level employees only given access under specific circumstances.

**Rule 3 - C2 INTERNAL**

Any information that must circulate only within the Company or one of its units is classified as C2 INTERNAL.

Such information can only be circulated only on a need-to-know basis. Criteria for assessing whether information is classified as INTERNAL include whether its unauthorized disclosure would:

- cause distress to individuals
- violate appropriate commitments to maintain the confidentiality of information provided by third parties
- violate legal restrictions on information disclosure
- cause potential financial loss or loss of profit, or facilitate improper profit
- give an unfair advantage to individuals or companies
- prejudice the investigation or facilitate crime commission
- disclose OST sh.a. regulations as well as the manner and organization of its internal activities

Most of the organization's employees are likely to handle "INTERNAL" information during their work day.

**Rule 4 - C1 PUBLIC**

Any information for which it has been decided that it can be made public and whose disclosure does not harm OST sh.a. interests is classified as C1 PUBLIC. Such classification concerns most of the company held information which is available to the public through established means of publication.

Documents containing C1 PUBLIC information shall not be assigned any owner nor will they be inventoried. However, it may be necessary to be aware of information falling into this classification over time, as circumstances may change and the need may arise to provide increased protection of previously public information assets.

**5.1 Rules on use (information classification perimeter)**

**Rule 5 - Initial classification**

Internal information, which is in the process of being created and is not classified by its owner, is automatically classified as "C2-INTERNAL".

However, information that is "C3-CONFIDENTIAL" or "C4-RESTRICTED" must be classified at the level required after creation by its owner and must not be COPIED on a USB, CD-ROM or DVD.

**Rule 6 - Marking**

All means of information communication must, at least, contain a mark the classification level of the information it contains.

This marking must, at least, specify the information classification level and comply with the marking requirements associated with that classification level (list of information recipients, validity date for its classification level, etc.).

Exceptions may exist in cases where information is presented in documents or tools whose format does not allow special characters, regulatory statements that use formats required by regulatory authorities or tax authorities, etc.

**Rule 7 - Change of lower / higher classification level**

Any modification of the confidentiality classification level is the responsibility of the person making the change.
Any information possessor may change the classification level when he/she deems it necessary. The owner considers the protection needs in light of the new context and informs each guardian of the change in level.
The information holder acting under his/her own responsibility, has the same rights as the possessor, except for information classified C4 RESTRICTED, for which the possessor has sole responsibility for a change in classification.

**Rule 8 - Classification of information outside OST sh.a.**

Any information coming from outside the company must be classified according to the protection required by the sender. In this case, the recipient becomes the "**de facto**" information owner, with all the obligations associated with this capacity.

## 6. Roles and responsibilities in the process of information classification and confidentiality protection

Responsibilities in the information classification structure and confidentiality protection are as follows:

### 6.1 Information possessor

The information possessor, who is characterized by his/her function or mission, is the main actor in this process. He is responsible for:
- Selecting the appropriate level of confidentiality classification as a function of the potential risk to the company caused by any release of said information;
- Compliance with the accompanying rules for use;
- Compliance with the use of related safeguards.

### 6.2 Director of the Department, Director of the Directorate and Head of the sector

The Director of the Department, the Director of the Directorate and the Head of the sector are responsible for monitoring and implementing the rules for information classification and confidentiality protection by their staff.

### 6.3 Directorate of Corporate Affairs (DCA)

DCA staff duties in cooperation with the relevant directorates:
- Participate in determining the goals and methods for classifying information confidentiality;
- Assist in the definition and updating of methodological tools that help classify information (guidelines, procedures, illustrative list of common documents with their suggested classifications, etc.);

- Define and update procedures and solutions for information protection;
- Perform actions to increase awareness of the rules for information classification and protection;
- Assist information possessors and superiors, at their request, in the field of information classification and protection;
- Contribute to the integration of the process goals and results for the information classification and protection in the risk management measures related to the information systems security, and in the risk analysis performed on a regular basis under their responsibility.

## 7. Information classification, documentation table

| | C1 PUBLIC | C2 INTERNAL | C3 CONFIDENTIAL | C4 RESTRICTED |
|---|---|---|---|---|
| **Definition** | Any information whose release does not harm the company interests or one of its subjects is classified as C1 PUBLIC | Any information that should circulate only within the Company or one of its units is classified as C2 INTERNAL | Any information that should be communicated only to persons concerned directly and whose unwanted disclosure could damage a company project, activity or entity is classified as C3. | Any information, whose disclosure could cause serious damage to the company's vital interests or to one of its branches, is classified as C4-RESTRICTED. |
| **Identification** | Marked as "C1 Public" | Marked as "C2 INTERNAL" | - Marked as "C3 CONFIDENTIAL" and owner of information<br>- Indication of the list of names of persons authorized to access such information | - Marked as "C4 RESTRICTED" and information possessor.<br>- List of authorized persons' names to access such information<br>-Disclosure strictly limited to recipients specified on the distribution list.<br>-If possible, mentioning of the information about the date and retention period for the classification level, as well as the lowest level after that. |
| **Printing** | No specific rules | No specific rules | Dedicated printer if possible or if not possible, the nearest network printer. The document must be removed from the printer as soon as possible by the information possessor. | Dedicated printer or other printer whose physical access is strictly limited to persons who need to know the information. |

| | | | | |
|---|---|---|---|---|
| **Distribution** | No specific rules | - Limited circulation on a need-to-know basis. External circulation to trusted partners is possible when covered by a formal confidentiality agreement (contractual clause for compliance with the protection rules of this instruction) | - Mandatory encryption of information using measures approved by DCK/SPSI<br>- Circulation within a clear list of persons (appointed or not).<br>- Transmission/circulation to a specific group of original rights' holders is carried out under the responsibility of the information owner.<br>- External circulation to trusted partners is possible when covered by a formal confidentiality agreement (contractual clause for compliance with the protection rules of this instruction). | - Mandatory encryption of information using measures approved by DCK /SPSI<br>- Circulation in a clear list of individuals.<br>- Transmission / circulation to a specific group of original rights holders requires the agreement of the information possessor.<br>- External circulation to trusted partners is possible when covered by a formal confidentiality agreement (contractual clause for compliance with the protection rules of this instruction). |
| **Duplication / Photocopying** | No specific rules | No specific rules | It is carried out under the responsibility of the owner or custodian who accepts the risk. | - Enabled or officially authorized by the information owner. Mandatory marking and identification of the custodian of the additional copy. |
| **Disclosure / Posting** | No specific rules | No specific rules | Sent in a double envelope (sealed; no open envelope window). The inner envelope is marked C3 CONFIDENTIAL. | Delivered personally by the owner to the recipient, or, failing that, delivered to a trusted person in a double envelope, with the inner envelope marked as C4 RESTRICTED. |
| **Storage/ archive** | No specific rules | No specific rules | Stored in a cabinet that must be locked. | Either kept in a safe or in an armored cabinet; Or stored under lock in secure, segregated areas, access to which is restricted to the owner and persons who need to know. |

| | | | | |
|---|---|---|---|---|
| **Storage / archive on fixed media** | No specific rules | No specific rules | - Encryption is recommended using SPSI approved measures<br>- Strengthened access control enabling access only to authorized persons (authentication by identification and authentication elements: password, smart card, biometric information, etc.)<br>- Archiving of physical media in secure areas designated for this purpose (with authentication access rights). | - Occupant encryption of information using SPSI approved measures<br>- Access control enabled only by authorized persons (authentication by identification elements and authentication: password, smart card, biometric information, etc.).<br>- Archiving of physical media in secure areas designated for this purpose (with authentication access rights). |
| **Storage/Archiving on removable media** | No specific rules | No specific rules | - Encryption is recommended using SPSI approved measures<br>- Physical media stored in protected areas, under the responsibility of the custodian or owner. | - Mandatory encryption of information using SPSI approved measures (removable disk, USB key, PDA, etc.).<br>- Physical media stored exclusively in secure areas designated for this purpose (with authentication access rights). |
| **Destruction** | No specific rules | No specific rules | Use of a paper shredder or deposit in a container that prevents retrieval of the document | Use of a paper shredder by the owner or custodian. |
| **Examples** | - Advertising (after the campaign has started).<br>- Documents intended to inform the public.<br>- Reviews and press prints. | - Internal directories and catalogs.<br>- Price list, invoices and supplier conditions.<br>- Training materials, instructions and procedure manual. | - Privileged information in the regulatory sense<br>- Customer information (account statements, organizations, projects, strategy, customer identity information)<br>- Content of personnel files (salaries, bonuses, social benefits)<br>- Speculative reports and internal audits<br>- Supervisory authorities reports<br>- Backup plans<br>- Project design (up to launch)<br>Space maps | - Company quarterly results before the publication of the accounts<br>- Evaluation and summary of provisions<br>- Documents related to acquisition projects, mergers, combinations, merging activities of large units<br>- Password backups<br>- Reports on persons suspected of fraud |

*The above examples are provided for illustration purposes only; the information owner remains his/her own judge and is responsible for attributing the confidentiality level on the information as a function of its true content. The relevant Directorate/Sector in cooperation with the Archive Sector must prepare the documentation list that OST produces and receives from third parties, determining the classification level for each document/information in*

*such a way that every employee in the capacity of owner has a clear classification what he/ she will do, taking into account the requirements of the law on the energy sector, the law on the right to information (public information) as well as the requirements of various regulatory acts that require transparency and the publication of various information by the OST during the exercise of his/ her activity.*