**NOT SECRET**

**Defradar Technologies**

**Operational Security Procedures – General Description**

© COMPANY NAME

Subject to legal provisions, no part of this document may be reproduced, adapted or redistributed, under no shape and using no means, in the absence of the prior written agreement of COMPANY NAME.

**NOT SECRET**

**Review and signatures page**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Author | .... | | | | |
| Author position | Risk & BCP Manager | | | | |
| Edition | 1 | | | | |
| Review | 0 | 1 | 2 | 3 | 4 |
| Date | 11.07.2011 |  |  |  |  |

**Document pre-approval**

| **Name** | **Pre-approved Ed. / Rev.** | **Position** | **Date** | **Signatures** |
| --- | --- | --- | --- | --- |
|  | 1/0 | SIMS Manager |  |  |
|  | 1/0 | ISC Manager |  |  |
|  | 1/0 | Infrastructure Management Team Leader |  |  |
|  | 1/0 | Systems Administrator |  |  |

**Document pre-approvals**

| **Name** | **Approved Ed. / Rev.** | **Position** | **Date** | **Signatures** |
| --- | --- | --- | --- | --- |
|  | 1/0 | General Manager |  |  |

**Document modifications**

| **Date** | **Author** | **Ed. / Rev.** | **Change reason** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Document distribution**

| **Name** | **Position** |
| --- | --- |
| COMPANY NAME | All staff |

**NOTE: The edition is modified when the structure of the document is radically modified or after at the most 5 revisions. All chapters of the new edition are initially issued in 0 revision.** **CONTENTS**

[1. ADMINISTERING AND ORGANIZING SECURITY 5](#_Toc510513574)

[1.1. General description 6](#_Toc510513575)

[1.2. Authorities involved in COMPANY NAME security 6](#_Toc510513576)

[1.3. Security operating mode of SIC COMPANY NAME 10](#_Toc510513577)

[1.4. Administrative procedures 10](#_Toc510513578)

[1.5. Reporting security incidents 10](#_Toc510513579)

[1.6. Drafting the security and acknowledgement procedures 11](#_Toc510513580)

[1.7. Procedures for controlling the technical staff access and for maintenance outside COMPANY NAME 11](#_Toc510513581)

[1.8. Procedures regarding private property electronic equipments and devices 12](#_Toc510513582)

[1.9. Risk management 12](#_Toc510513583)

[1.10. Audit 12](#_Toc510513584)

[2. PHYSICAL SECURITY 12](#_Toc510513585)

[2.1. COMPANY NAME’s security environments 12](#_Toc510513586)

[2.1.1. Global security environment (MSG) 12](#_Toc510513587)

[2.1.2. Local security environment (MSL) 13](#_Toc510513588)

[2.1.3. Electronic security environment (MSE) 13](#_Toc510513589)

[2.2. Areas designed for installing SIC COMPANY NAME’s equipments 14](#_Toc510513590)

[2.3. Locks keys and combinations 14](#_Toc510513591)

[2.4. Verification procedures when finishing working hours 14](#_Toc510513592)

[2.5. Control of staff access to COMPANY NAME locations 15](#_Toc510513593)

[2.6. Control of equipment access to COMPANY NAME locations 15](#_Toc510513594)

[3. PERSONNEL PROTECTION 15](#_Toc510513595)

[3.1. Authorized users of COMPANY NAME SIC 15](#_Toc510513596)

[3.2. COMPANY NAME SIC Personnel 16](#_Toc510513597)

[3.3. Personnel security training 16](#_Toc510513598)

[3.4. Restricted access within the COMPANY NAME spaces for persons who do not have any access authorization 17](#_Toc510513599)

[4. INFORMATION SECURITY 17](#_Toc510513600)

[4.1. Transferring information from/to the COMPANY NAME SIC 17](#_Toc510513601)

[4.2. Storing documents 18](#_Toc510513602)

[4.4. Storage environments records 18](#_Toc510513603)

[4.5. Marking documents and tagging storage environments 18](#_Toc510513604)

[4.6. Archiving and destroying documents and storage environments 20](#_Toc510513605)

[5. INFOSEC 20](#_Toc510513606)

[5.1. Hardware security 20](#_Toc510513607)

[5.2. Software security 21](#_Toc510513608)

[5.3. Identifying users 22](#_Toc510513609)

[5.4. Users authentication 23](#_Toc510513610)

[5.5. Using the electronic mail service 23](#_Toc510513611)

[5.6. Using the remote VPN service 24](#_Toc510513612)

[5.7. Using the Internet service 24](#_Toc510513613)

[5.8. Access to FileServer 25](#_Toc510513614)

[5.9. Backups 25](#_Toc510513615)

[5.10. Errors (system dropdowns) 26](#_Toc510513616)

[5.11. Antivirus protection 26](#_Toc510513617)

[5.12. Automated security management and audit 26](#_Toc510513618)

[5.13. Cryptographic configuration 27](#_Toc510513619)

[6. CONFIGURATION MANAGEMENT 27](#_Toc510513620)

[7. PLANNING MEASURES FOR EMERGENCY SITUATIONS IN ORDER TO CONTINUE THE ACTIVITY AND DISASTER RECOVERY 28](#_Toc510513621)

# 1. ADMINISTERING AND ORGANIZING SECURITY

## 

## 1.1. General description

1. On COMPANY NAME level, the Operational Security Authority (AOS COMPANY NAME) administers and organizes security (including the whole set of operational policies and procedures).
2. COMPANY NAME’s IT&C system (SIC COMPANY NAME) consists of an extended area computer network built on its own communication support or that of authorized providers, with access points in various locations belonging to the organization.
3. The purpose of SIC COMPANY NAME is to provide:

* An integral component of the business, production and service process helping the organization win a competitive advantage;
* Interconnecting users with the organization, to enable communication and collaboration between locations and departments within COMPANY NAME;
* Support for developing the business on maximum efficiency level.

## 1.2. Authorities involved in COMPANY NAME security

1. The COMPANY NAME’s Operational Security Authority   
   (AOS COMPANY NAME) is responsible for organizing, administering and implementing all security measures meant for the performance and functioning of COMPANY NAME.
2. AOS’s general responsibilities are following:

* Coordinating activities for enabling the security of classified information stored or processed in the specific security area;
* Inspects locations belonging to COMPANY NAME from a global, local and electronic security environment point of view;
* Performs security controls for testing the implementation of security measures on COMPANY NAME level;
* Evaluates results from performed security tests;
* Drafts operational security procedures (PrOpSec) on COMPANY NAME level;
* Develops and updates internal classified information protection norms;
* Coordinates and regulates the internal activity in the field of information protection in all departments within COMPANY NAME;
* Informs COMPANY NAME management regarding potential threats, vulnerabilities and security risks and proposes measures to prevent, eliminate or reduce their effects;
* Organizes activities to train staff involved in the information management process within COMPANY NAME;
* Develops the analysis of the impact on COMPANY NAME’s mission;
* Develops plans for continuing the activity for each location within COMPANY NAME;

1. AOS COMPANY NAME’s organization chart and components are established via an internal decision of COMPANY NAME management, with following being the dedicated functions:
   1. Manager of AOS COMPANY NAME – is also the security responsible;
   2. Security administrator;
   3. System administrator;
   4. COMSEC administrator;
   5. Security administrator in the location area.
2. Those nominated to be part of AOS COMPANY NAME are approved for access to classified information at least of SECRET level.
3. The same person cannot fill in the system administrator and security administrator positions at the same time. Those assigned on these positions can also have other work tasks, cumulated with those assigned for AOS COMPANY NAME.
4. AOS components

***a. AOS COMPANY NAME Leader***

The leader of AOS COMPANY NAME answers for all activities in the responsibility area – refer concretely to following responsibilities:

* Is the security responsible for COMPANY NAME, with specific attributions for the area in which classified information is managed;
* Coordinates activities performed by the staff appointed with responsibilities, according to below mentioned functions;
* Monitors the application and controls how procedures defined in technical and security documents are performed;
* Verifies and evaluates the activity performed by staff nominated in AOS concerning ensuring SIC COMPANY NAME performance and security;
* Identifies the organization’s security risks and periodically analyzing these risks;
* Identifies possible risk scenarios, defining and proposing preventive measures;
* Verifies, develops and implements security measures for reducing risks;
* Develops, implements and maintains security controls;
* Performs investigations related to security incidents;
* Drafts reports following performing security controls/investigations;
* Maintains an awareness program over information security within COMPANY NAME (specific meetings/presentations, security guides, educative brochures, etc.);
* Drafts new security policies and procedures (in order to improve existing ones and adapt to new technological and legal challenges);
* Performing simulation exercises specific for the Activity Continuity and Disaster Recovery Plan (PCA-DR)
* Permanent collaboration with all department managers and experts nominated to be part of intervention teams detailed in PCA-DR;
* Monitoring the compliance regarding respecting information security as well as risks systems and information in the company are subject to.

1. ***Security administrator***

SIC COMPANY NAME’s security administrator coordinates how security measures approved and implemented within the system are applied and respected and has following responsibilities:

* Takes part to developing, updating and implementing SIC COMPANY NAME’s security policy;
* Responsible for selecting, implementing and maintaining security measures within SIC COMPANY NAME;
* Participates to developing and updating SIC COMPANY NAME security documentation;
* Provides consultancy regarding SIC COMPANY NAME performance under security conditions;
* In order to identify any unauthorized access attempts or other hardware or software malfunctions, centralizes reports regarding verifying journal and audit files created by ASZL;
* Verifies the existence and means of respecting security measures meant to enable activity continuity in emergency situations;
* Participates to investigating security incidents, security breaches or attempts to break SIC COMPANY NAME security;
* Fills in the SIC COMPANY NAME security incidents tracking registry;
* Takes part to providing management for the SIC COMPANY NAME configuration;
* Verifies if all users with access to the system have corresponding access rights for information processed in SIC COMPANY NAME;
* Notifies AOS leader of all anomalies regarding SIC COMPANY NAME’s security.

1. ***COMSEC Administrator***

The COMSEC administrator of SIC COMPANY NAME coordinates the identification, implementation and updating of security measures for IT networks and has following responsibilities:

* Coordinates activities regarding making the communication infrastructure available in the administration of the ICT department, used by SIC COMPANY NAME;
* Provides consultancy regarding the safety of communication equipments belonging to SIC COMPANY NAME;
* Monitors meeting approved security measures for performing the equipment maintenance and repair activity;
* Proposes implementing hardware, firmware and software modifications and improvements of communication equipments in SIC, in order to make sure that there are no breaches in the SIC COMPANY NAME security;
* Keeps track of communication equipments in SIC COMPANY NAME, their hardware, firmware and software changes, modifications and flaws;
* Verifies the corresponding application of security measures in the COMSEC field;
* Informs the AOS leader in case some events or incidents take place regarding community security in SIC COMPANY NAME and takes part to their investigation;
* Participates to developing and updating the security documentation belonging to SIC COMPANY NAME, for those parts that concern him/her;
* Cooperates with the security administrator and the system administrator in order to ensure the security of SIC COMPANY NAME.

1. ***System administrator***

SIC COMPANY NAME’s system administrator answers for the operational and security management of technical systems (usually Desktop) with maintenance, diagnose and HelpDesk role for stations in the internal network and has following responsibilities:

* Ensures implementing SIC COMPANY NAME’s security policy;
* Provides optimum equipment exploitation in accordance with requirements approved with the security documentation;
* Updates operating systems and the software installed with security-related improvements (hot fixes, patches, service packs);
* Administers its own applications and data bases and provides integrity, efficiency and a secured work environment in the internal network;
* Implements the antivirus software and ensures its periodical update for all equipments;
* Participates to developing and updating the system’s security documentation;
* Participates to developing proposals for performing some hardware and software modifications for improving the system’s security;
* Cooperates with COMSEC’s security administrator and with its administrator in order to ensure SIC COMPANY NAME’s security;
* Participates, upon request from the AOS leader, to investigating security incidents occurring at SIC COMPANY NAME;
* Notifies the AOS leader concerning any malfunctions regarding SIC COMPANY NAME’s functioning.

1. ***Security administrator in the location area (ASZL)***

ASZL answers for the operational and security management of the administered location and fulfills following attributions:

* Develops, submits for pre-approval and pre-approval location specific work procedures;
* Develops, submits for pre-approval and pre-approval the Activity Continuation Plan (PCA-DR) specific for the location it administers, created according to the model provided by AOS management;
* Ensures that safety measures mentioned in security policies and procedures specific to its area of responsibility are implemented;
* Ensures the exploitation of services and equipments installed in the responsibility area in optimum conditions and in accordance with existing security requirements;
* Monitors the fulfillment of approved security measures for performing the maintenance and repair of equipments in the location area, which it writes down in specific registers;
* Informs the security administrator and/or AOS leader about any security breach or incident noticed, as well as about any modification generated by the staff dynamics or possible internal reorganizations;
* Participates to trainings organized by AIOS and provides training for users regarding operational security procedures within SIC COMPANY NAME;
* Is the PCA-DR coordinator specific for the location it administers from a security point of view.

1. SIC COMPANY NAME users, whose main responsibilities are:

* To participate to trainings organized by department managers, ASZL and the security officer;
* To know and meet security procedures and rules approved for work stations and their application norms for SIC COMPANY NAME;
* To know and meet security procedures and rules approved for work stations and their application norms for the departments they are part of;
* To know and meet provisions of procedures implemented for the security of personal character data (DCP);
* To correctly classify and manage information received under according security conditions;
* To sign the “Agreement regarding processing DCP” and the “Agreement for maintaining data confidentiality”, to correctly classify and manage information received under according security conditions;
* To immediately report any breach or incidents regarding the security to ASZL or the security officer, as well as any other issues significant from a SIC COMPANY NAME security point of view.

## 1.3. Security operating mode of SIC COMPANY NAME

1. The security operating mode of SIC COMPANY NAME is “HIGH LEVEL”, operating mode where ALL persons with access right to the COMPANY NAME system are authorized for the highest classification level of information stored, processed or transmitted to SIC, and access to information is differentiated, according to the “need to know” principle.

## 1.4. Administrative procedures

1. There is an internal computerized network interconnected to the central network within each location belonging to COMPANY NAME.
2. Disconnecting from SIC can be the result of a AOS decision, by previously sending a notification in this respect to the ASZL administering that location, following:

* Not respecting measures approved in the security documentation;
* The occurrence with new security risks of unacceptable level;
* Not meeting measures approved via the security documentation;
* The occurrence of a security incident and not meeting procedures regarding addressing security incidents;
* Reorganizing the location or the system.

## 1.5. Reporting security incidents

1. Security incidents can be grouped as follows:

**a) major incidents** – those incidents referring to any of the following cases:

* Developing or possible sabotage actions;
* Breaches of security rules with the result of compromising confidential information;
* Discovering significant vulnerabilities in SIC, intrusion detection systems, fire detection and extinguishing systems or any other physical or electronic systems;
* Significant incidents caused by malicious software that can affect another SIC or that may activate other malicious software unknown types or versions;
* INFOSEC incidents overlapping the area of competence of the location SIC belongs to;
* Incidents object to IT crime;
* Incidents caused by natural catastrophes, accidental or caused by staff negligence, affecting COMPANY NAME’s security, staff and/or assets.

**b) regular incidents** – those incidents concerning any of the following cases:

* INFOSEC incidents that are not part of the major incidents category;
* Isolated incidents caused by known malicious software;
* Breaches of security rules that are not part of the major incidents category;

1. In case a major incident is discovered, following activities must be performed at once:

a) the person discovering the major incident must report this immediately to the ASZL;

b) ASZL communicates the AOS security administrator by phone and the specifically filled in form shall be forwarded within 24 hours from finalizing the incident research;

c) the security administrator communicates the incident to the AOS leader that disposes the immediate initiation of the research together with all responsible AOS members, depending on the nature of the incident;

e) as soon as the causes of the incident have been determined, the AOS leader forwards at the soonest the filled in form with measures taken in order to remedy the incident and/that is to be implemented to COMPANY NAME management.

1. Regular incidents must be investigated locally under direct AOS coordination and is registered by ASZL in the Security Events Registry. Details regarding this type of individual incidents need not be communicated to COMPANY NAME management, but they must be centralized and periodically communicated to management in order to be an analysis topic.

## 1.6. Drafting the security and acknowledgement procedures

1. Security Procedures (PrSec) for each location within COMPANY NAME are framework documents issued by AOS COMPANY NAME that are to be implemented according to requirements mentioned by AOS COMPANY NAME in the document “COMPANY NAME System Specific Security Requirements (CSS SIC COMPANY NAME)”.
2. PrSec are created in two copies, and after being pre-approved by AOS members, they are sent to COMPANY NAME management to be approved. ASZL keeps a copy, and another one can be found at the AOS leader.
3. ORNISS, SRI as well as DGIPI for certain projects where it is required to issue some industrial security certificates perform evaluations regarding how security measures for the area where classified information is managed are implemented and met.
4. AOS members shall perform evaluations regarding how security measures for all other areas are implemented and met, according to their responsibilities.
5. AOS COMPANY NAME representatives accompany ORNISS, SRI respectively DGIPI representatives in security inspections organized for the classified information area.
6. ASZL must provide staff training, together with the AOS leader, regarding existing security procedures and implemented security measures.
7. The staff training activity is written down in the training chart specific for each employee and filled in the training plan.
8. COMPANY NAME staff shall only acknowledge specific PrSec stipulations depending on the access level, meeting the “need to know” principle.

## 1.7. Procedures for controlling the technical staff access and for maintenance outside COMPANY NAME

1. The access of technical and maintenance staff in the locations area within COMPANY NAME is possible with ASZL approval, and identification information is highlighted in the location’s Visitor Registry.
2. Throughout the activity, technical and maintenance staff is accompanied by the ASZL or by a nominated person.

## 1.8. Procedures regarding private property electronic equipments and devices

1. It is forbidden to bring any other electronic information storage devices to the SIC COMPANY NAME terminal operating area, except for those approved by the AOS.
2. It is forbidden to bring any other electronic information storage devices to area where classified information is managed, except for those approved by the security officer.
3. It is forbidden to use private equipments or devices for storing or processing electronic information in the area where SIC COMPANY NAME terminals function.

## 1.9. Risk management

1. AOS COMPANY NAME has an inspection for verifying each location within COMPANY NAME at least once a year as well as any time notified of modifications inflicted upon existing conditions.
2. After finalizing verification inspections, AOS COMPANY NAME develops a new risk analysis report and determines what measures are necessary in order to minimize risks and prevent acknowledged vulnerabilities.

## 1.10. Audit

1. Audit refers to those activities performed in order to monitor events regarding SIC COMPANY NAME’s security.
2. The system’s audit records are consulted by the security administrator within AOS, in order to identify possible failed attempts to access SIC COMPANY NAME.
3. Any failed attempt to access the system or information is reported to the AOS leader and also to the security officer for systems managing classified information.

# 2. PHYSICAL SECURITY

## 

## 2.1. COMPANY NAME’s security environments

### 2.1.1. Global security environment (MSG)

1. For COMPANY NAME, the global security environment consists of the proximity of buildings where the company performs its activity.
2. Ensuring the global security environment is the responsibility of building administrators with the permanent involvement of the AOS leader and the ASZL in order to forbid unauthorized access and includes following measures:

* Physical barrier protecting the limits of the office;
* Intrusion detection systems;
* Access control (electronic, electro-mechanic or using other means);
* Security using specialized staff;
* CCTV and security lights.

1. In order for persons to access MSG they must be identified; visitors are identified and their identification data is registered in access control registries; they are accompanied throughout their visit and their activity takes place in the presence of organization staff.
2. Outside working hours and off days, access to the MSG is forbidden, buildings are locked and security 24/24.
3. The AOS leader and ASZL cooperate with building administrators in order to implement security measures mentioned in the COMPANY NAME Specific Security Requirements document in order to ensure the security of that location.

### 2.1.2. Local security environment (MSL)

1. The local security environment consists of the rooms where COMPANY NAME performs its activity.
2. The area where equipments belonging to COMPANY NAME are installed is at least “administrative area” level.
3. Access to rooms designed for equipments connected to the COMPANY NAME network is limited and allowed only for staff running activities in that area, appointed by organization management.
4. Access to the room where SIC COMPANY NAME equipments are installed is controlled using specialized systems.
5. Terminal locations are equipped with smoke/fire alarms and extinguishing devices;
6. Work stations are placed so as to:

* Prevent the unauthorized view of information by placing the monitor screen against access doors in the classified information area.
* Prevent placement near possible flooding sources.

### 2.1.3. Electronic security environment (MSE)

1. The electronic security environment is defined by significant security limits of SIC COMPANY NAME in electronic or processing context.
2. Each work station has options for performing audit and log on recordings active.
3. Audit records are kept for six months and verified monthly.
4. The COMPANY NAME network is secured by using following technologies and equipments:
   1. SSL/TLS-type technologies
   2. IPSEC VPN-type technologies – encrypting traffic
   3. VLAN-type technologies – logical separation of networks
   4. Statefull inspection-type technologies – access to distribution servers is filtered using a firewall
   5. Antivirus-type technologies – the mail server has an antivirus server integrated, that scans all messages, both those received and those sent.
5. Protection measures and mechanisms are implemented for the servers’ security, aiming at:
   * Access control using a username and a password at least 8 characters long;
   * Impossibility for system users with limited rights to access by deactivating shell accounts on the server;
   * Logging all events on server level, the AOS security administrator sending and monitoring their status;
   * The system administrator periodically auditing log files;
   * Weekly updated antivirus protection;
   * Providing availability of all functions and services by configuring machines in 1+1 regime.
6. In order to provide server maintenance, monthly or every time needed, the communication system is paused, having previously sent a notification to all users connected to the system via e-mail.
7. It is forbidden to use the Internet as means of disseminating classified information.
8. Unused ports of system equipments are deactivated.
9. MSG, MSL and MSE are detailed and materialized on PrSec level for each location.

## 2.2. Areas designed for installing SIC COMPANY NAME’s equipments

1. Equipments for SIC COMPANY NAME are located in areas as follows:

* Class II security area – for classified information and Data Center;
* Administrative area – for equipments within other locations.

1. When entering security and/or administrative areas, a warning message such as the below is displayed:

***ATTENTION !***

***ACCESS ALLOWED ONLY FOR AUTHORIZED STAFF***

## 2.3. Locks keys and combinations

1. Rooms where equipments designed to connect to SIC COMPANY NAME are installed have locks or electronic access systems. For each point of presence there is a record of the staff that had the key enabling access into the room or the electronic system enables viewing this list.
2. Spare keys are kept according to the location’s internal regulations, by concern on the ASZL, so as to know who took them and who handed them over, date and time.

## 2.4. Verification procedures when finishing working hours

1. IT systems’ users are obliged to terminate the work session by using “Log off” or “Look” every tome leaving the work station.
2. When ending the work day, the last person to leave the room must verify the locks, doors and windows in the rooms, turn off any electrical lighting, verify and take all necessary measures in order to eliminate fire causes, as well as the integrity of seals where the case.

## 2.5. Control of staff access to COMPANY NAME locations

1. Staff with access to COMPANY NAME locations is decided by the organization’s management in an internal decision, a copy of it being saved by the AOS leader.
2. COMPANY NAME locations can be accessed based on the nominal credential and access card.
3. Visitors or maintenance persons entering COMPANY NAME locations for various reasons are permanently accompanied by an authorized person.
4. It is forbidden that unauthorized staff accesses the equipments or acknowledges documents listed or existing in electronic format.

## 2.6. Control of equipment access to COMPANY NAME locations

1. ASZL drafts and keeps a list of approved equipments to be in his/her responsibility area.
2. The list of equipments contains the name of the equipment, the type, series, level of classification of processed information, place it is kept, staff authorized to access it.
3. It is forbidden to replace equipments in the approved list without having notified the AOS leader or staff especially nominated to manage equipments.
4. It is forbidden to bring or use equipments or devices enabling to store or send electronic data in the area where classified information is managed, except for those approved by the security officer.

# 3. PERSONNEL PROTECTION

## 

## 3.1. Authorized users of COMPANY NAME SIC

1. ASZL, users, likewise the personnel benefiting from classified documents and who have access to the area of the terminal on which classified information is being stored, must fulfill the following conditions:
   * + ASZL is authorized to access information at least classified as “WORK SECRET”;
     + Users and personnel who benefit from classified documents are authorized to access at least “WORK SECRET” classified documents, depending on their access level;
     + Complies with the “need to know” principle.
2. Approval for accessing classified information is obtained according to the legal procedures from ORNISS.
3. Need to know, for classified information, is established by the management of the organization through an internal decision, a copy being kept by the ASZL.
4. THE AOS manager, likewise ASZL holds a copy of the list with the personnel authorized to receive and process the respective documents.
5. ASZL, likewise the authorized personnel for documents evidence, distribute classified documents only to persons found on the list approved by the organization management.
6. Each user with access right to the COMPANY NAME SIC terminals has a personal account which can be accessed based on username and password.
7. The access to the KOON portal is done only by users authorized based on a user account, created by the IT department and a password established by the user after the account was created.
8. Main users obligations:
   * + To know and comply with the operational procedures and security regulations approved for workstations and their application regulations for the COMPANY NAME SIC, depending on the approved level of access;
     + To know and comply with the provisions of the “Security and infrastructure and ITC services use Policy”, “The Users Backup Policy”, “The Policy for Accessing the FileServer”, “The Incidents reporting procedure and IT requests”, “The Procedure for using the antitheft system”, “*Remote Access VPN Procedure*”; “The action procedure in case of fire”**.**
     + To know the “Information security confidentiality policy”, the „Security policy for processing personal information” and sign the „data confidentiality agreement”, respectively „The agreement regarding the processing of personal information”**.**
     + To manage, in security conditions, the information received through the COMPANY NAME SIC;
     + To immediately notify ASZL regarding any breach or incidents regarding the security of the system which it finds or any other significant problems from a COMPANY NAME SIC security point of view.

## 3.2. COMPANY NAME SIC Personnel

1. Persons authorized to access COMPANY NAME SIC are:
   1. COMPANY NAME AOS Manager;
   2. Security Administrator;
   3. System Administrator;
   4. COMSEC Administrator;
   5. Location Area Security Administrator (ASZL);
   6. Authorized COMPANY NAME SIC operators;
   7. The authorized administration and maintenance personnel of the COMPANY NAME SIC;
   8. Other persons assigned by the organization management, through internal decision, as users of the system.
2. Persons nominated for managing the COMPANY NAME AOS have the necessary rights required to access classified information and to at least SECRET classification levels.

## 3.3. Personnel security training

1. AOS COMPANY NAME ensures the annual preparation and is imposed each time AZSL requests it.
2. ASZL ensures the possibility to train the personnel who works within the responsibility area.
3. For each location, the training is done each time a new user is assigned and a system access account is created.

## 3.4. Restricted access within the COMPANY NAME spaces for persons who do not have any access authorization

1. In order to diminish the risk of compromising classified or confidential information, visitors access to COMPANY NAME spaces is limited.
2. If a visitor is approved by the organization management to access COMPANY NAME spaces, ASZL is notified.
3. Visitors are recorded within the evidence register, specially drafted and they are accompanied during their entire visit period.
4. The responsibilities of the person accompanying the visitor are:
   * + To accompany the visitor from its entry in the building and for his entire route, directly to the area where the activity shall take place;
     + To verify if the visitor is registered within the visitors Register and if it has approval for accessing the respective spaces;
     + To monitor the visitor during his entire visiting period;
     + To ensure that during the visit, the respective visitor does not use any recording devices, storage environments, mobile phone within the area in which classified information can be found and for the Data Center;
     + To ensure that the room where the visitor shall be located does not include any classified information;
     + To ensure that their monitors have a screen saver set;
     + At the end of the visit they must accompany the visitor until he/she exists the building.

# 4. INFORMATION SECURITY

## 

## 4.1. Transferring information from/to the COMPANY NAME SIC

1. The information received through the COMPANY NAME SIC is saved by users on a server within the specially assigned folder “*Users backup policies*” and “*FileServer Accessing Procedure*”.
2. Classified information is stored within a special area, accredited by ORNISS according to the internal protection regulations of the classified information.
3. The distribution of classified information is done according to the “need to know” based on a specific access authorization.
4. It is forbidden to delete classified messages or documents from the system without the prior approval of the security operator.
5. Periodically, documents can be saved on storage environments, labeled and stored within the classified documents evidence compartment.
6. It is forbidden to transmit IFC or IFE information from the COMPANY NAME SIC, to unauthorized persons, or through systems which are not certified at the same classification level of the information.
7. Listing or saving on electronic storage environments is done by authorized operators and recorded within the special dedicated register.
8. The information from the COMPANY NAME SIC are listed only to dedicated printers, based on a nominal access card, in compliance with the internal regulations.
9. IFC/IFE drafted based on classified documents shall have the confidentiality level of the initial documents according to the national regulations (HG 585/2002).
10. The transformation of IFC in IFE is done only on special dedicated scanners, which are monitored.
11. The transformation of classified IFC in classified IFE is done based on the approval of the security operator, based scanners authorized by ORNISS.
12. The IFE transfer in the system is preceded by the antivirus verification operation.

## 4.2. Storing documents

1. Organization documents are stored in closets/lockers found within the rooms where the COMPANY NAME personnel perform its daily activity.
2. Classified documents are stored in security containers found within a room authorized by ORNISS.

## 4.4. Storage environments records

1. The storage environments of the information, used for saving or transferring classified information are taken into evidence within the storage environments logs, kept within an authorized location.
2. Storage environments include special tags/labels which contain the registration number and classification level.
3. Storage environments are taken over by users based on signature within the evidence register.
4. Storage environments dedicated for classified information cannot be used for storing other information.

## 4.5. Marking documents and tagging storage environments

1. Marking documents and tagging storage environments used within the COMPANY NAME is done depending on the classification level of the included information.
2. Within the COMPANY NAME, the following types of information are processed, stored and transmitted:

|  |  |  |
| --- | --- | --- |
| **CONFIDENTIALITY CATEGORY** | **CONFIDENTIALITY CLASS** | **CONFIDENTIALITY LEVEL** |
| NON-CLASSIFIED INFORMATION | PUBLIC | NON-SECRET |
| SENSITIVE INFORMATION | PRIVATE | CONFIDENTIAL |
| CLASSIFIED INFORMATION | WORK SECRET | WORK SECRET |
| STATE SECRET | SECRET |

Category – **NON-CLASSIFIED INFORMATION**

* Class – **PUBLIC DOCUMENTS**:
  + **NONSECRET**
    - Information accessible to any user from and out of the company.
    - *Marking and evidence:* It doesn’t require any marking or special evidence; they are documents, data or information obtained from public sources.
    - *Authorization:* Access must not be authorized.
    - *Dissemination:* is not restricted.

Category – **SENSITIVE INFORMATION**

* Class – **PRIVATE** documents:
  + **CONFIDENTIAL (color code – Model: RGB, Red: 0, Green: 176, Blue: 240)**
    - Such information, due to their importance are accessible only to a restricted number of authorized persons, which must not be made public and which can be used within the company by the employees; Such information can be distributed to company partners after concluding confidentiality agreements with them.
    - *Marking and evidence*: marked CONFIDENTIAL or not, these documents, data or processed information, stored or handled within the company, shall be considered CONFIDENTIAL and shall be evidenced according to the internal regulations.
    - *Authorization*: Only authorized employees of COMPANY NAME have access to such documents according to the “need to know” principle.
    - *Dissemination*: Their dissemination must be evidenced within the internal records (Input/output register).
    - This category includes but is not limited to the following types of information:
      * *Employees contact information;*
      * *Company policies, procedures and regulations;*
      * *Internal communications specific to the company;*
      * *Information regarding the list of suppliers of the company;*
      * *Personnel file of the employees, organizational chart and payment sheets;*
      * *Data regarding company clients;*
      * *Development plans;*
      * *Financial data which have not yet been published;*
      * *Company business plans.*

Category – **CLASSIFIED INFORMATION**

* class – **WORK SECRETS** documents:
  + **WORK SECRET (color code – Model: RGB, Red: 255, Green: 255, Blue: 0)**
    - *Marking and evidence*: it requires a special marking and evidence according to *the internal protection regulations for classified information*.
    - *Authorization:* All COMPANY NAME employees who perform their activity within WORK SECRET projects must have access authorizations to WORK SECRET information. The authorizations for accessing WORK SECRET are obtained from the Classified Information Office, according to the specific internal procedures.
    - *Dissemination*: Their dissemination must be evidenced within the WORK SECRET Information Evidence Register.
* **STATE SECRET**:
  + **SECRET (color code – Model: RGB, Red: 0, Green: 176, Blue: 80)**
    - *Marking and evidence*: it requires a special marking and evidence according to *the internal protection regulations for classified information*.
    - *Authorization:* All COMPANY NAME employees who perform their activity within SECRET projects must have access authorizations to SECRET information. The authorizations for accessing SECRET information are obtained according to the specifications from GD 585/2002, for approving national Standards for classified information in Romania.
    - *Dissemination*: The dissemination of SECRET information must be evidenced within the Evidence register of Secret and Strictly Secret Information.

## 4.6. Archiving and destroying documents and storage environments

1. The archiving of classified documents is done according to the national regulations regarding information protection.
2. The archiving of the confidential documents is done according to the internal regulations.
3. If it is necessary to replace the HDD which has been used for classified information, it shall be destroyed and/or deleted by using a certified product, and the operation is executed based on the approval of the security operator, who receives his approval from the COMPANY NAME.
4. The operations regarding the destruction of the storage environments are recorded in a destruction report, approved by the security operator, in which the destruction method is presented, who performed the operations and the date of the operations.
5. The destruction report is stored according to the internal regulations regarding information protection.

# 5. INFOSEC

## 

## 5.1. Hardware security

1. Authorized users of the COMPANY NAME SIC are obliged to know and comply with the work procedures and electronic equipments.
2. The IT department is responsible for a correct installation, maintenance and modification of the settings of the hardware components.
3. ASZL is responsible with the physical security of the equipments and permanently verifies their condition.
4. Hardware equipments on which classified information are stored is marked with the messages warning on the maximum classification level of the information circulated.
5. The communications route through the buildings is evidenced, and this task belongs to the IT department.
6. It is forbidden to move the equipments in other location without the notification of the AOS manager and without the approval of the COMPANY NAME management.
7. It is forbidden to remove the equipments of the COMPANY NAME SIC from the installation area, except for force majeure cases, when it is necessary to act according to emergency situations action plans.
8. Equipments maintenance/repairing is done by the authorized personnel within the IT department or maintenance companies, under the direct surveillance of the personnel assigned for security for the area in which classified information are managed – without removing the equipments from their designations.
9. If for performing certain maintenance works or for remedying certain defects it is necessary to remove an equipment from the COMPANY NAME locations and if it contains a storage environment which was not used for processing or storing classified information, it is mandatory that the storage environment to be removed from the equipment and stored by the security operator in a B category safe.
10. In order to avoid possibilities of recovering certain classified information from the remaining memories of the equipment, they shall be overwritten through the following procedure:

* Memories are removed from the equipment;
* Are installed in a similar bun unused equipment for processing classified information and not connected to other systems;
* Various applications are launched in execution and unclassified data are used for processing on the equipment running the memories;
* The equipment is restarted, repeating the previous operations for at least three cycles;
* The equipment is stopped and memories are pulled out and reinserted within the basic equipment.

## 5.2. Software security

1. Approved computer applications to be installed on all the terminals connected to the COMPANY NAME network are:

* Windows XP SP3, Vista, Windows 7 Operating systems;
* MSOffice applications suite;
* Adobe Acrobat Reader;
* Software antivirus;

1. The software installed is licensed and ensured by the IT department.
2. It is forbidden to install other categories of software except the ones approved and installed by the IT department.
3. It is forbidden to install the personal software on the workstation connected to the COMPANY NAME SIC
4. When accessing the terminals, users are warned by the following message:

IT IS AN OFFENSE TO CONTINUE WITHOUT AUTHORIZED ACCESS!

This system is restricted.

Individual unauthorized access attempts shall be punished. If you are not authorized, terminate the access!

By clicking OK you accept the information presented above.

1. When accessing the terminal on which classified information are published, users are warned by the following message:

WARNING!

An authorized terminal is accessed for processing classified information.

Unauthorized use cat attract disciplinary measures, contraventions, civil or penal if applicable.

1. The terminals sessions blocks after 15 minutes of inactivity, and they can be unblocked by inserting the password.
2. The operating system is updated with the necessary improvements regarding security (hot-fix-es, patch-es, service-packs) only by the specially assigned personnel within the IT department.
3. Firewalls are implemented based on the principles of minimalistic and minimum privileges, being thus configured:
   * + Records all the applications blocked through the security policy;
     + Refuses the output traffic which cannot be generated by internal addresses;
     + Refuses the entire traffic generated by invalid source addresses;
     + Refuses the traffic from external sources which might be generated by internal addresses;
     + Reassembles the fragments in full packages before applying the security policy of the firewall.
4. For preventing and detecting intrusions or other cybernetic attacks to its address, the COMPANY NAME SIC benefits from specific services, ensured by the IT department. The events within the COMPANY NAME network are logged and stored for a period of 6 months. The mechanism which collects data is syslog, the events being transmitted to a central syslog server from which they are processed, normalized and prioritized. Based on the priorities of the events, operators notify the system Administrator within the COMPANY NAME AOS for repairing noticed problems. ASZL and the other AOS members notify through the system Administrator the occurrence of certain events or cybernetic attacks to the COMPANY NAME SIC.
5. IT departments ensure and monitor the operation of the equipments within the entire network through specialized NOC departments (Network Operation Center).
6. Within the Exchange servers, all messages are scanned with various licensed antivirus/antispyware/antispam engines.

## 5.3. Identifying users

1. All persons with access to the COMPANY NAME SIC are identifiable and authorized.
2. Email addresses are created on the SIC email server of COMPANY NAME, corresponding to each user connected to the system ([**lastname.name@company-name.ro**](mailto:lastname.name@company-name.ro)).
3. The operating systems of the terminals control the access of the system users based on the user ID and password, which are verified during the connection.
4. Each user with access rights to the SIC terminal of COMPANY NAME within the organization has a personal account on the computer connected to the system assigned by a username and password.
5. Only the IT department can establish and configure the accounts of the authorized users.
6. Only the persons authorized from within the It department have access to the administrator account.

## 5.4. Users authentication

1. The operating systems of the terminals control the authenticity of the users’ passwords.
2. Users passwords fulfill the following conditions:

* Are changed once every 2 months;
* Lower and Upper cases must be used, numbers, special characters which are accepted by the authentication mechanism;
* The length of the passwords must be of at least 8 characters;
* They have no logical significance or identity;
* When changing the password, a different password from the previous 5 ones must be chosen (passwords history -5)

1. It is forbidden no write the password or transmit it to other persons.
2. Workstations connected to the COMPANY NAME network have been configured with BIOS passwords established by the IT department.
3. Workstations connected to the COMPANY NAME network are configured for activating the screen-saver after 5 minutes of inactivity and by inserting the password.

## 5.5. Using the electronic mail service

1. The electronic mail service (email) of the COMPANY NAME must improve the services towards the organization clients, through a better internal and external communication and altogether for reducing IFC. Employees using the electronic mail system of the organization must adhere to the following policies and procedures:
2. Must be used for business purposes only;
3. All the information created, sent or received through this service, including all email messages and electronic files are the property of the organization;
4. Users must ensure that the correct email address of the addressee is written within the To… box;
5. Any message of file transmitted through e-mail must include the name of the employee;
6. Using other personal email accounts is forbidden without the prior approval from the management;
7. The access within the organization network from other networks using the communications infrastructure of other Internet providers is not allowed until the express authorization of the organization management and until they are not appropriately protected by the firewall or other software/hardware security devices of the organization;
8. Confidential information must not be transmitted through e-mail without being encrypted, using software/hardware devices agreed by COMPANY NAME;
9. Classified information ARE NOT transmitted through the electronic mail
10. Email messages must contain an appropriate and professional language – it is forbidden to distribute racist messages which might discriminate, include pornographic elements, obscene or with other offenses;
11. Using the email system of the organization for personal purposes or other purposes than business without the prior agreement of the organization, is forbidden;
12. Forwarding confidential messages of the organization to external locations is forbidden;
13. It is forbidden to broadcast personal points of view regarding social events, politics, religion or other events which are not related to the organization business;
14. It is forbidden to transmit, via the email, commercial or publicity materials which have not been requested.

## 5.6. Using the remote VPN service

1. VPN remote access to the local LAN network of the company is based on a request certified by the hierarchic manager of the persons requesting access and approved by the ICT Department manager, according to the internal procedure.
2. ICT Networking supplies, configures and verifies the software (Cisco VPN Client) for VPN access to the COMPANY NAME network and the IT infrastructure configures the remote access rights of the user in Active Directory and archives the VPN remote access request in compliance with the requirements of the company, signed and approved by all concerned persons.

## 5.7. Using the Internet service

1. The IT department authorizes and approves the Internet connections used within the organization and takes care of the operations related to protecting the Internet access connections through current firewall operations.
2. All organization users who have access to the Internet must comply with the provisions expressed in IT security policies and act in compliance.
3. All internet connections or connections to other private networks must be authorized and approved by the IT department. Users shall access the internet through the internet connection supplied in their department by the It department of the organization.
4. Any other additional connection must be authorized and approved by the IT department. These auxiliary connections may be, but not limited to:
5. Data modems or any other communication device which allows internet connection or to other networks;
6. Wireless access points.
7. The internet must be used according to the following aspects:
8. All employees must use the internet access in business purposes and for their current activity;
9. All employees must use the internet access in compliance with the legal provisions in force;
10. The use of the internet connection by the users is monitored and recorded;
11. The organization does not have any control on the information accessed by the users on the Internet and on its content, thus, the organization does not assume any responsibility regarding the information accessed by its users and their content;
12. Any software or files downloaded via the internet through the organization network, become the property of the organization; any such downloaded element must be used by the employees in compliance with the licensing and use rights afferent;
13. The organization reserves its right to temporarily or permanently block the access to certain sites, services or even suspend the internet connection;
14. Any file downloaded from the internet, before being opened must be scanned with the antivirus protection software of the organization.
15. Using the internet within the organization for the following reasons is not allowed:
16. Access, upload, download or distribution of pornographically materials or with sexual content;
17. Violating enforced rules;
18. Vandalizing or destroying the individual or organizational property;
19. Invading the private right of other;
20. Violating use rights or the use of the copyrights without any permissions;
21. Using them for financial or commercial gain;
22. Degrading or interrupting the overall performance of the network;
23. Introducing within the organization network if any software form or other malware materials

## 5.8. Access to FileServer

1. Accessing the FileServer is done based on the “need to know” principle, including folders created for each department which can be accessed only by the persons within the department, according to the access rights granted by the manager of the respective department, except to the **0\_Corporate\_Info** folder which includes general interest information, available to all employees.

## 5.9. Backups

1. Backups for public or private documents (Unclassified or Confidential) are done according to the backup policy for users**.**
2. For realizing the backup strategy in terms of COMPANY NAME, the following aspects have been considered:

* Where shall the backup environments be stored;
* Which data should be backed up;
* How often should the backup be performed;
* How fast can the backup environments be accessed when an unwanted event occurs
* Who is authorized to have access to backup environments;
* Where shall the backup environments be delivered;
* Who shall restore the data from the backup environments;
* Which is the main scheme for tagging backup environments;
* For how long shall the backup environments be stored;
* When backup environments are stored within the backup location;
* What measures are taken for their safety.

1. Quarterly, or any time necessary, the security administrator saves the audit records and the implemented security policy.
2. Backup copies are stored in different locations, in adequate security conditions according to the requirements of the organization and in order to be accessed in emergency situations.
3. Backup copies for classified documents are saved on storage environments which are appropriately marked and registered, used for backups and for storage within security containers (B type) in ORNISS authorized rooms for managing classified information.

## 5.10. Errors (system dropdowns)

1. If certain malfunctions are detected within the servers, standalone workstations or connected to the COMPANY NAME network, only the IT department takes measures to replace them and reestablish the connection to the system.

## 5.11. Antivirus protection

1. All workstations and servers within the IT infrastructure of the organization, standalone or connected to the COMPANY NAME network, physical or virtual machines, use the antivirus program approved by the ITC department, which complies with the following rules:
2. The antivirus program must NOT be deactivated in any way, exceptions shall be approved by the ITC department;
3. The installation, configuration, modification or deletion of the antivirus programs is done by the ITC department;
4. The configuration of the antivirus program must not be modified in a manner which restores the efficiency of the program;
5. The frequency of the automated updates of the program is scheduled by the IT Department it must not be modified in any way;
6. Any notification of the antivirus program from a workstation or server must be immediately notified to the IT department by the user reporting it.

## 5.12. Automated security management and audit

1. The security administrator is obliged to activate the automated audit system of the terminals operating systems and set them for logging journals.
2. Audit records of the systems shall be recorded monthly, or any time necessary, by the security administrator or by an assigned person, in order to determine unsuccessful system access attempts and are stored for at least 6 months.
3. The verification of audit records is registered by the security administrator within the events log.
4. Any unsuccessful attempt to access the system or to information shall be communicated to the AOS managed and to the COMPANY NAME management.
5. The security manager is obliged to configure the operating systems installed on workstations in order to record the printing activity performed by the printers which are not endowed with own monitoring systems and manage this activity.
6. Audit reports, specific to Windows operating systems, installed on terminals within SIC COMPANY NAME supplies the following information:

* The date and hour of the event;
* The type of the event;
* The origins of the events;
* Successfully opening work sessions by users;
* Unsuccessful attempts for opening a work session and user accounts where the attempts have been tried;
* Methods of using passwords and their modification;
* Abnormal termination of a work session;
* Other abnormal events, including work outside schedule hours;
* Performing activities which can modify, avoid or interrupt security facilities controlled by the operating system.

## 5.13. Cryptographic configuration

1. The COMSEC administrator of AOS COMPANY NAME is responsible for all the security aspects of the communications and SICS cryptography of COMPANY NAME, in compliance with the security policies specific to the field.
2. For each location, ASZT answers with the security of the communications equipments associated to terminals and the physical security of the communications support.
3. Assigned users are responsible with the safe management of the certificate token issued by the DigiSign Certification Authority.

# 6. CONFIGURATION MANAGEMENT

1. The SIC configuration management of COMPANY NAME is done by the IT department, with the AOS involvement and consists in identifying, controlling, evidencing and auditing all the modifications within the hardware and software configuration of SIC.
2. ASZL from each location is responsible with the hardware and software configuration of the equipments installed within the responsibility area.
3. If it is necessary to modify the configuration of the submission location of the equipments, ASZL shall immediately notify the AOS manager and/or the IT department manager.
4. The SIC configuration management of COMPANY NAME includes the implementation of various security measures:

* During the entire life cycle of the system, hardware and software configuration modifications are performed by specialists of the ITC department, after notifying the AOS and the previous approval of the organization management;
* The security administrator and the system administrator hold a copy of the complete inventory for SIC equipments found in their responsibility, likewise a detailed scheme of the hardware and software configuration;
* Any modification of the hardware and software configuration of the system equipments shall be recorded by the security administrator and/or system within the equipments files;
* all system equipments shall be marked appropriately (afferent to a system and the classification level, by case);

1. The security administrator and the system administrator shall execute, at least an annual control of the hardware and software configuration, activity which is logged within the “Events log”.
2. The AOS manager can organize unscheduled controls of the system hardware and software configuration in order to verify if other resources are used, beside the approved ones, or other modified software versions.
3. It is forbidden to perform any modifications to the hardware or software configuration of the workstations used for fulfilling work tasks.
4. Discovering methods or suspicions regarding the modification of the hardware or software configuration of the workstations must be acknowledged by ASZL, which shall notify the security administrator and/or AOS manager in order to verify the system configuration in emergency regime.
5. Any major modification of the configuration or the establishment location of the system equipments shall determine the appropriate modification of the security documentation.

# 7. PLANNING MEASURES FOR EMERGENCY SITUATIONS IN ORDER TO CONTINUE THE ACTIVITY AND DISASTER RECOVERY

1. The measures plan for continuing the activity and disaster recovery (PCA-DR) establishes the procedures for restoring operations, resources and specific services of COMPANY NAME in case special situations which result in deactivating locations/departments from within COMPANY NAME.
2. PCA-DR for the locations/departments within COMPANY NAME apply to resources and IT services which must be reestablished in emergency situations and are applied to positions, operations and SIC resources for reestablishing their operational condition.
3. In emergency situations, ASZL acts according to the PCA-DR provisions.
4. The PCA-DR coordinator is assigned by the COMPANY NAME management after the proposal of AOS and has the following contributions:

a) Performs, together with the Operational Security Authority (AOS), the analysis of the impact on specific location activities, for:

* Identifying critical resources of the informational and communications systems (SIC);
* Identifying the impact and maximum allowed time for stopping the activity of the respective location;
* Establishing priorities regarding the reestablishment of resources and SIC services.

b) Collaborates with AOS for identifying the implemented security measures.

c) Drafts, in collaboration with AOS, the strategy for reestablishing SIC resources and services establishing:

* backup method;
* The necessity of a backup location, the type of the location and its coordinates (if applicable)*;*
* Priorities in replacing equipments;
* Types of intervention teams in emergency situations, the number and the responsibilities of its members;
* Optimal costs for implementing the strategy.

d) Drafts the PCA content, specific to the managed location, based on the PCA model provided by AOS, forwarding for approval to the management of the COMPANY NAME, after it was previously approved by the AOS management.

e) If an emergency situation occurs, he shall proceed to activating the approved PCA and will notify the managers of the appropriate intervention teams, according to the established notification chain.

f) Drafts, together with AOS, the PCA testing plan, through theoretical and practical exercises and coordinates the performance of these exercises.

g) Distributes to intervention team members, with the AOS approval, PCA copies or extras, while also keeping the evidence of the number of PCA copies and persons to whom they have been distributed and withdraws the pages of the extras or plan copies which have suffered modifications, replacing them with the new ones.

h) Keeps permanent updated evidence, as a table, regarding the participation of the intervention team members to the periodical training sessions.

i) Ensures the training of replacements for basic intervention team members, likewise new members assigned for these teams.

j) Analyzes and updates, if applicable, the PCA testing plan, at least once a year or each time significant modifications of the location mission and structure occur for the location they administrate, recording the modifications within the Modifications Evidence Register.

1. PCA-DR specific to each location within COMPANY NAME takes place as a result of the security risks analysis performed by AOS and the impact analysis on the specific activities regarding the ASZL location.
2. Annually, the security operator for the classified information area and ASZL, together with the AOS management, ensures the verification of the evacuation and reestablishment measures of the connection to COMPANY NAME and to update PCA-DR.
3. Testing PCA-DR, training the personnel and performing periodical exercises are basic elements in terms of the viability of the ability to continue the activities in emergency situations and to identify PCA-DR deficiencies, contributing to the evaluation of the personnel abilities, with responsibilities in applying the provisions of the plan, thus implementing the approved procedures more efficiently and rapidly.
4. When testing PCA-DR the following fields shall be considered:

* Reestablishing SIC services using backup copies, including within a backup location;
* Internal and external communications;
* SIC performances when using backup equipments;
* Rebuilding the operational state of SIC;
* Notification procedures for activating PCA-DR.

1. Testing the efficiency of the plan takes place by performing periodical testing exercises for PCA-DR elements, which consist of:

**a) Theoretical exercises** – these are the exercises based on hypothetical situations, and the personnel having responsibilities in the application of PCA-DR and which participates to such exercises presents exposures regarding PCA-DR procedures which it has to follow and the action method for applying procedures. Theoretical exercises take place before the practical exercises.

b) **Practical exercises** – are concrete exercises, concentrated on PCA-DR elements. These sorts of exercises include real simulations of various emergency situations and sometimes to certain major crisis situations.

1. Exercises include the real testing of how to act when restoring SIC to the backup location, with the removal or not of the basic SIC from operation.
2. Planning the performance of the exercise is notified to the participants so that the members of the teams involved providing the necessary time in order to prepare and correlate current activities with the ones imposed by the exercise.
3. Training intervention teams members with responsibilities in applying PCA-DR is an activity which completes the field of PCA-DR testing and must take place once every 6 month with the entire personnel involved.
4. The PCA-DR coordinator has evidence consisting of a table regarding the attendance level, certified through signature and updated permanently. Also, the PCA-DR coordinator ensures the training of new members assigned within the intervention teams.
5. The training of the entire PCA-DR personnel must reach a specific level, so that team members are able to act without the necessity to read procedures, thus becoming a priority objective of the training activity.
6. The personnel with responsibilities in applying PCA-DR is trained in the following fields:

* Plan scope and objectives;
* The collaboration and communication method between assigned intervention teams;
* Procedures applied in emergency situations;
* Reporting procedures;
* Requirements for maintaining SIC security;
* Notification/activation procedures, used for reestablishing SIC resources and services and the system restore stages, specific to each team;
* Individual responsibilities of teams members, both in terms of notifying/activating, reestablishing resources and SIC services, likewise during system restore stages.

1. Conclusions resulted after the performances of the exercises consist in the main elements to be used when updating and improving PCA-DIR provisions.