Eversted

Information Security Policy

Eversted

Information Security Policy

S.C. FILTRE AER CURAT S.R.L.

Table of Contents

PURPOSE

The purpose of this Policy is to implement the measures required for the adequate security of information systems and the protection of personal data to European standards in order to avoid security incidents and ensure the necessary protection of personal data and the rights of individuals to privacy, as well as to avoid damage of the Company image, as a result of the vulnerability of information systems

SECURITY OF INFORMATION SYSTEMS

The security of the information system must be a responsibility assumed by the management structures of S.C. FILTRE AER CURAT S.R.L. .

The management structures must ensure a clear and properly managed direction to achieve the objectives set by the security policy, taking into account the following elements:

a) reviewing and approving the security policy and establishing responsibilities related thereto;

b) monitoring significant changes in the exposure of the information system to threats
major;

c) review and monitoring of security incidents of the information system;

d) approval of measures to increase information security.

In order to establish and maintain security policies, it is essential to involve relevant professionals in making decisions on the security of the information system.

Access to information processing equipment of S.C. FILTERS AER CURAT S.R.L. by third parties must be supervised. For third party access, a risk assessment should be performed to establish security implications and control requirements.

Protective measures must be agreed upon and included in a contract with third parties. Also, outsourcing agreements/ contracts should address security risks, controls and procedures for computer systems, networks and/ or office equipment. All assets of the information system should be accounted for and have a designated officer. Asset liability helps to ensure that proper protection is maintained. The person responsible for an element of the information system must be able to be identified for all major assets and have responsibilities for maintaining and implementing appropriate controls. Responsibilities for control may be delegated.

The information shall be classified to indicate the priorities and degree of protection required. The information has varying degrees of sensitivity and importance, some of which require additional level of protection or special handling. An information classification system should be used to define an appropriate set of levels of protection, as well as the need to establish special handling measures.

In order to reduce the risk of human error, theft, fraud or abuse of confidence, security responsibilities must be implemented from the recruitment stage, included in the employment contracts, and monitored during the workplace activity. All the employees of the company or third parties who have access to the information system of S.C. FILTRE AER CURAT S.R.L. should sign a confidentiality agreement.

To ensure that users are aware of information security threats and are prepared to support organizational security policy in the course of their work activity, the employees of the company or third parties should be trained in security procedures and the correct use of information processing systems.

All security incidents must be reported, and an effective and rapid security incident reporting system should be implemented for this purpose, to be acknowledged by all employees.

Critical or sensitive business information must be stored in secure locations, protected within an appropriate security perimeter, with appropriate security barriers and access controls. They should be physically protected against unauthorized access, damage, and interference. The protection offered must be proportionate to the risks identified. IT&C equipment must be physically protected against security threats and environmental hazards.

Responsibilities and procedures for managing and operating all information processing systems should be established. This implies the development of instructions for use and incident response procedures approved by the company management and acknowledged by all staff.
S.C. FILTRE AER CURAT S.R.L. Precautions are needed to prevent and detect the introduction of malicious software. Software and computing equipment are vulnerable to the introduction of malicious software, such as viruses, network worms, Trojan horses. Users should be aware of the dangers of unauthorized or malicious software and managers should, where appropriate, introduce special controls to detect or prevent the introduction of malicious software. In particular, it is essential to take precautionary measures to detect and prevent infection with computer viruses of employees' computers. Routine procedures should be established for performing strategic backups, periodic simulation of restoration on copies

achieved, logging of the events and defects, where possible the permanent monitoring of critical equipment. Information and software exchanges between organizations should be controlled and should be in accordance with the legislation in force. Procedures and standards to protect information and data in transit should be established and initialed in agreements signed by all parties involved.

MEASURES REQUIRED TO SECURE INFORMATION SYSTEMS

PHYSICAL SECURITY

Inventory of authorized and unauthorized equipment

A common practice of criminal groups is to use the techniques of continuous scanning of the IP addresses of the target organizations, aiming to connect new and/ or unprotected systems, or laptops with definitions or outdated security packages (patches) due to the fact that are not frequently connected to the network. One of the common attacks takes advantage of newly installed systems that are not configured and secured in terms of security packages until the next day, being easily identified and exploited through the Internet by attackers. As for the computer systems inside the protected networks, attackers who have already gained access can target and compromise those systems that are insufficiently or inappropriately secured.

The S.C. FILTERS AER CURAT must pay particular attention S.R.L. to equipment and systems that are not included in the inventory of organizations, such as various personal mobile devices, test systems, etc. and which are not permanently connected to the network. Generally, these types of equipment tend not to be properly secured or have no security controls that meet the security requirements. Even if this equipment are not used to process, store or access critical data or information, once they are networked, they can provide attackers with access to other resources and a point where advanced attacks can be launched. Maintenance by S.C. FILTRE AER CURAT S.R.L. of an accurate and current inventory, controlled by active monitoring and configuration management, may reduce the chances for attackers to identify and operate unprotected systems. The inventory procedures establish the owners of information and information systems, documenting the responsibilities for maintaining the inventory for each component of the systems.

Also, S.C. FILTRE AER CURAT S.R.L. can use passive resources identification tools (which "passively" listens at the network interfaces the equipment that announces the presence by modifying the traffic). These monitoring and inventory tools should include functionalities such as:

- Identification of new unauthorized equipment connected to the network within a predefined time frame;

  Alert or send notification messages to a predefined list of clerical staff
- Isolation of the unauthorized system;
- Identification of the location where the connection was made.

Inventory of authorized and unauthorized applications and operating systems

Criminal groups use address space scanning techniques of targeted organizations to identify vulnerable versions of software that can be remotely exploited. Such attacks can be initiated by distributing hostile web pages, documents, media files and other types of web content through their own web pages or other trustworthy web pages. Complex attacks can also be zero-day, exploiting vulnerabilities the same day or before they are publicly known. Without proper knowledge or control of the implemented software, S.C. FILTRE AER CURAT S.R.L. cannot provide the necessary protection for IT resources. Inventory capacity and inadequate control over the software that are installed and authorized to run on the equipment of the organizations, make these computer environments more vulnerable. Such inadequately controlled equipment is liable to execute software that is not required for the specific nature of the activity, inducing potential security breaches or running malware-induced programs after the system has been compromised. Once equipment has been operated, it is often used as a starting point for subsequent attacks and for gathering sensitive information from the compromised system and other systems connected to it. Vulnerable equipment are used as launching points for "advancement" in the network and partner networks. Organizations that do not use the complete inventory of software packages will fail to discover the systems running vulnerable or malicious software and further reduce problems or attacks. Commercial software and specialized tools for inventorying computer resources are widely used to facilitate simultaneous verification of applications used in organizations, extracting information about the level of update packages of each software program installed to ensure the latest version is used. Monitoring systems used by S.C. FILTRE AER CURAT S.R.L. should also include functionalities such as:

- Ability to identify unauthorized software by detecting attempts to install or execute it;
- Alert administrative staff within a predefined time frame;
- Block installation prevent execution or quarantine.

Wireless equipment control

In the absence of effective security measures implemented for wireless networks, attacks can be initiated aiming mainly at stealing important data for any type of organization. As wireless networks do not require direct physical connections, wireless equipment provides attackers with a convenient vector for gaining access to the target environment.

Developed attack techniques can be initiated from outside, avoiding organizations' security perimeters. Thus, portable equipment can be infected by remote exploitation as long as they are removed from the security perimeter outside the organization and then used as back doors once returned to the organization and reconnected to the network.

Protective measures against attacks carried out through wireless networks are aimed at the use of both scanning, detecting, and discovering network tools and intrusion detection systems. S.C. FILTRE AER CURAT S.R.L. must capture the wireless traffic carried out in the perimeter areas to determine if more permissive protocols for transmission or encryption are used than those required. In addition, remote management tools can be used within networks to collect information about the wireless capabilities of devices connected to managed systems. The instruments used shall include the following functionalities:

- ability to identify authorized device configurations or unauthorized wireless devices within the organization's coverage area and which are connected to these networks;
- identification of new, unauthorized, newly connected wireless devices;
- alerting administrative staff; ▫ identifying the area and isolating the network access point.

Network security design

Security measures, even well implemented in computer systems, can be circumvented in poorly designed networks. Without a properly planned and implemented network architecture, attackers can bypass security measures from different systems, penetrating the network to gain access to the target systems. Attackers frequently target network maps to identify unused connections between systems, improper filtering, and non-segregated networks. Therefore, a robust and secure network can be achieved through implementation by S.C. FILTRE AER CURAT S.R.L. of a process that provides the necessary security measures. In order to ensure a robust and easy to secure environment, the architecture of each network must be based on models that describe its overall structure and the services it offers. S.C. FILTRE AER CURAT S.R.L. should document charts for each network in which the network components with the significant groups of servers and client systems are highlighted.

Limitation and control of network ports, communication protocols and services

Attacks can also be launched through remote accessible network services that are vulnerable to exploitation. Common examples include improperly configured web servers, email servers, file and print services, DNS servers pre-installed on a variety of devices, often without taking into account the business need for the services offered. Many software packages install and start services as part of the basic package installation without informing the user or administrator that the services have been activated. The attacks follow the discovery of accounts, passwords or codes through scans and attempts to exploit the exposed services.

Such types of attack can be prevented by using port scanning tools to determine which services are "listening" to the network for a number of target systems. To determine open ports, the scanning tools can be configured to identify the protocol version and the service that "listens" on each open port discovered. The services discovered and their versions are compared with the inventory of services required by S.C. FILTRE AER CURAT S.R.L. for each equipment.

Protection of perimeter areas (or boundary defense)

Attacks can be focused on exploiting systems that can be accessed from the Internet, including DMZ (term derived from "Demilitarized Zone", also known as "perimeter networking"), as well as client systems (workstations, laptops) that access Internet content through the perimeter area of the network.

The attack techniques launched by the criminal groups use the weaknesses in the configuration or architecture of the perimeter, the network systems, and the client equipment to gain initial access within the organization. Once the access is obtained, the attackers will penetrate deeper into the network for the purpose of stealing or exchanging information or establishing a basis for subsequent attacks against domestic host systems. In many cases, attacks occur between networks of business partners, sometimes referred to as "extranet", the attacks moving from one organization's network to other organizations' networks, exploiting vulnerable systems hosted on extranet perimeters. In order to control the flow of traffic through the perimeter networks and to provide the records for the detection of attacks on compromised systems, the protection of the perimeter areas must be multi-layered, using equipment and applications Firewall, Proxy, DMZ networks, prevention systems and IPS and IDS network intrusion detection, as well as filtering traffic sent to or received from the networks.

Intrusion prevention and detection systems for S.C. FILTRE AER CURAT S.R.L. at perimeter level must include the following features:

- have the ability to identify unauthorized/ illegitimate packages sent to or received from a secure area;
- blocking unauthorized/ illegitimate packages;
- alerting administrative staff.

Physical access to locations

Ensuring an adequate security environment starts right from the physical access to the buildings/ spaces/ locations of the SC FILTRE AER CURAT S.R.L. that need to be protected.

In order to make the guard and defense systems more efficient against unauthorized penetration, the physical security measures should be included in a Physical Security Plan, and the implementation of these measures should be based on the principle of "deep defense", with the aim of establishing:

- the space to be protected;
- external security devices designed to delimit the protected area and discourage unauthorized access (perimeter fence, physical barrier that protects the boundaries of the location, guarding specialized personnel);
- security intermediary devices designed to detect attempts or unauthorized access to the protected area (IDS intrusion detection systems, lighting, closed circuit television - CCTV);
- some internal security devices designed to delay the actions of potential intruders (control of electronic, electromechanical access or through other means).

Control of the access of personnel of S.C. FILTRE AER CURAT S.R.L. in the protected areas is carried out by security personnel or by electronic systems, taking into account the following:

- the access of each employee is made through specific places, based on the access permit;
- the access permit can clearly specify the identity of the issuing organization or the place where the holder has access, but this aspect is not recommended for the areas where they are managed

classified information (Practically at the level of each legal entity that manages classified information

additional rules on access can be established);

- for the access of the employees of the contracting companies that carry out various works of repair and maintenance of the buildings or maintenance, the beneficiary organizations will issue, on the basis of the identity documents, at the request of the authorized representatives of the agents concerned, temporary access documents.

The physical security plan includes the description of all the physical security measures implemented for the protection of the locations and can be structured as follows:

- delimiting, marking, and configuring the areas that need to be protected; □ the guard and defense□system; warning and alarm system;
- control of access, keys, and digit combinations;
- the mode of action in emergencies; □ how to report, investigate and record the breach of security measures;
- responsibilities and implementation of physical security training and training measures;
- responsibilities and means of carrying out checks, inspections, and controls of security system;
- additional physical protection measures.

Logical security

Hardware configurations for mobile devices, workstations and servers

On both Internet and domestic networks already compromised by attackers, automatic cyber-attack programs are constantly searching for target networks to find systems that have been configured with vulnerable software installed. The default configurations are often oriented to facilitate the operation, use of the systems, but they are not secured and leave useless services usable in their default state. This way the attack techniques try to exploit both the services accessible via the network and the client's navigation software.

Protective measures against these attack techniques include the acquisition of system and network components with security configurations already in place, the installation of pre-configured security systems, the updating of configurations periodically and their tracking within a configuration management system.

These measures can be implemented by the S.C. FILTRE AER CURAT S.R.L. by creating system images and storing them on secure servers along with the use of configuration management tools. Depending on the solution adopted, these tools can actively monitor deviations from the implemented configurations, providing the necessary information to ensure the use of the established configurations and will include the following functionalities:

- Identification of any changes/modifications within a secure image that may include changes to key files, ports, configuration files or installed software;
- Comparison of the image of each system with the official image securely stored within the configuration management system;
- Block the installation and prevent the execution along with the alert of the administrative personnel.

Security configurations for network equipment - Firewall, Router, Switch

Attackers take advantage of a common practice in configuring the security level on certain network equipment: users request temporary exceptions for specific business considerations, these exceptions are applied but not removed as soon as the business need disappears. In even more serious situations, the security risk of such an exception is neither properly analyzed nor evaluated in terms of necessity.

Attackers look for breaches in firewalls, routers and switches and then use them to penetrate the system. The attackers exploited the deficiencies of these network equipment to gain access to the targeted environments, to redirect traffic to another network or malicious system that advertises itself as a trusted system, and to intercept and alter information as they are sent. With such actions the attacker gains access to sensitive data, alters important information or even uses a compromised system to "pose as" another trusted network system.

Some organizations use commercial tools to evaluate the set of rules on network filtering equipment, in order to determine the extent to which they are consistent or conflicting.

S.C. FILTRE AER CURAT S.R.L. will do an automatic check of the status of the network filters and search for errors in the sets of rules or in the Access Control List (ACL) that could allow unwanted services on that equipment. Such tools should be used at every significant change to the rule set on firewalls, router ACLs or other filtering technologies. Minimum recommended functionalities to maintain optimal control at network equipment level:

- Identify any changes to network equipment, including routers, switches, firewalls, and IDS and IPS systems (any changes to key files, services, ports, configuration files, or any other software installed on the equipment
- The configuration of each system must be compared with the master database with images to verify any changes in configuration in terms of security impact.

Ways to protect against malware

Malicious software is a dangerous aspect of threats in the Internet environment, targeting end users and organizations through browsing, email attachments, mobile devices as well as using other vectors. The malicious code can interact with the content of the system, capture sensitive data, and spread to other systems.

Modern malware aims to avoid signature-based and behavioral detection and can disable anti-virus tools running on the target system. Anti-virus and anti-spyware software, collectively known as anti-malware tools, helps to defend against these threats by trying to detect malware and block their execution. Anti-malware tools, in order to be effective, require regular updates. Relying on user policies and actions to keep anti-malware tools up to date, they have been widely discredited because many users have not been able to consistently apply these tasks. To ensure regular and effective updating of anti-malware tools, solutions are used that automate these tasks. These solutions, also called end-point security suites, use integrated management features to verify the activity of anti-virus, anti-spyware and host-based IDS tools on each managed system. Daily or at predefined intervals, it runs automatic assessments and performs results reviews to identify systems that have deactivated protection tools, as well as systems that are not updated with the latest malware definitions.

In order to increase the security level for the protected systems, as well as for the systems that are not covered by the organizations management solutions, the network access control technologies are used, through which the equipment is tested in terms of compliance with the security policies before allowing the network access. Some organizations implement free or commercial honeypots and "lure" tools - known as "tarpit tools" to identify attackers in their environment.
S.C. FILTRE AER CURAT S.R.L. must permanently monitor these instruments to determine
when traffic is directed to attackers and connection attempts are made. Once identified

these events, security personnel must obtain the source of the addresses from which the traffic is generated

and other details associated with the attack to provide the data needed for the investigation activities.

Anti-malware tools will include the following features:

- Identification of malicious software installation, installation, execution or execution attempts execution attempts;
- Block the installation and prevent the execution or quarantine of malicious software when alerting administrative personnel.

Application security

Recent criminal group priorities include attacks on web-based application vulnerabilities as well as applications in general. Applications that do not check the volume of user-generated entries fail to "sanitize" the entries by filtering out character sequences that are unnecessary or potentially malicious or do not initiate the "cleaning" of variables properly, thus being vulnerable to remote compromise.

Attacks can be performed by "injecting" specific exploits including buffer overflows, SQL injection attacks, cross-site scripting, cross-site request forgery, and click code jacking to gain control over vulnerable systems.

In order to prevent such attacks, internally developed applications as well as third-party applications must be rigorously tested by S.C. FILTRE AER CURAT S.R.L. to identify security deficiencies. For third-party applications, S.C. FILTRE AER CURAT S.R.L. must ensure that suppliers have performed rigorous security testing for products, and for internally developed applications, S.C. FILTRE AER CURAT S.R.L. must perform security testing or employ specialized services to perform such tests. Tools testing source code or those for web application security scanning have proven useful for securing, along with penetration testing performed manually by specialists with extensive programming knowledge and application testing expertise.

Recommended features in the application security system:

- Detecting and blocking attack attempts at application level;
- Testing periodically, weekly, or even daily;
- Mitigate all high-risk vulnerabilities in web-accessible web applications - identified with vulnerability scanners, static scanning tools and scanning tools

review of automatic database configurations - either by changing the flow or by implementing a compensatory control.

Personnel security

Controlled use of administration privileges

A first method of attack in order to infiltrate an organization's network is the misuse of administrative privileges. Two common methods of attack take advantage of the lack of control over these administrative privileges: In the first method, a workstation user, using a privileged account, is tricked into opening a malicious attachment from the email, downloading and opening a file from a malicious website, or simply browsing a website hosting dangerous content that can exploit the browser. The file or exploit contains executable code that runs on the victim's machine either automatically or by persuading the user to execute the content. If this user account has administrative privileges, the attacker can completely take over the victim's system and install tools such as keystroke loggers or keyloggers (an app that holds everything typed in a file), sniffers (intercepts and decodes network traffic) and remote control software to identify administration passwords and other sensitive information.

Similar attacks also occur via email: an administrator opens an email containing an infected attachment, which is then used to obtain a network access point and to attack other systems. A second method is the elevation of privileges by guessing and "breaking" a password of an administrative account, in order to gain access to a target machine.

Whether administrative privileges are widely used within SC FILTRE AER CURAT S.R.L., the attacker will gain easier and faster control over the systems, as there are several accounts with administrative privileges to be tested. A common situation specific to such an attack is that of domain administrative privileges in complex Windows environments, with the attacker having significant control over a large number of machines and their data. An optimal management of the administrative accounts is achieved with a series of functionalities or activities such as:

- extracting the list of privileged accounts, both on individual systems and at the level of domain controllers, and periodically checking the list of active services if any browser or email service uses high privileges (the use of scripts looking for certain browsers, email services and programs document editing);

- administrative accounts can be configured to use a web proxy in certain operating systems and have no access to the e-mail application.
- Setting the minimum acceptable length of the password for example to 12 characters, setting a corresponding complexity algorithm.

Access control based on the "Need to Know" principle

Some organizations do not carefully identify and separate sensitive data from the least sensitive or publicly available on internal networks. In many environments, internal users have access to all or most of the information on the network. Once the attacker has penetrated such a network, they can find and transmit important information externally, without considerable effort.

Even in some situations of penetration in recent years, attackers have managed to gain access to sensitive data with the same access account as for ordinary data, stored on common servers.

It is vital that S.C. FILTRE AER CURAT S.R.L. to understand what its important information are, where they are located and who needs to access them. To reach the classification levels, S.C. FILTRE AER CURAT S.R.L. must review the key types of data and their importance at the organization level. This analysis can be useful in drawing up the scheme of classification of information throughout the organization. In the most common case, the classification scheme contains two levels: public (unclassified) and private (classified) information. Once the private information has been identified, it can be further subdivided into subclasses depending on the impact on the organization, if compromised.

What we can do to apply the principle as efficiently as possible:

- Data identification, classification by levels, correlation with business applications; network segmentation so that systems with the same sensitivity are on the same network segment; access to each network segment must be controlled by the firewall and possibly encrypted traffic on a network segment with unsecured access;
- Each user group or employee should have clearly specified in the job requirements what type of information they have to or need to access in order to perform their duties. Depending on the requirements of the job, access will be allowed only on the segments or servers required for each job. Each server should record the detailed logs so that access can be tracked and situations where someone accesses data that they should not have access to can be examined;
- The system shall be capable of detecting all access attempts without appropriate privileges and shall have alert capabilities.

Monitoring and control of user accounts

Attackers frequently discover and exploit legitimate user accounts but not used to impersonate legitimate users, making it difficult to detect the attack by the network security system. There are often cases where the user accounts of the contractors or employees who have completed the collaboration with the organization remain active. Moreover, current malicious or former employees have accessed old accounts long after the contract expires, maintaining access to the organization's systems and sensitive data for unauthorized and sometimes malicious purposes.

Monitoring and control of user accounts are activities of the administrative staff of S.C. FILTRE AER CURAT S.R.L. and have at least functionalities such as:

- Enable the logon function of the information related to the use of the accounts, thus configuring it to generate consistent and detailed data;
- Use of dedicated scripts or tools for log analysis so that the profile of access on certain systems can be evaluated;
- Account management, with more focus on inactive ones; □ The system must be capable to identify unauthorized user accounts when they exist on the system.

Skills assessment and security training

Every organization that is believed to be prepared to identify and respond effectively to attacks is responsible to employees and contractors to observe the deficiencies in knowledge and expertise, and to support their coverage through exercise and training. A robust skills assessment program can provide management with robust information about areas where security awareness needs to be improved and becomes useful in determining the optimal allocation of scarce resources in order to improve security practices.

Closely related to policies and awareness is the training activity of the staff of FILTRE AER CURAT S.R.L. . The policies communicate to the employees what to do, the training offers them the methods and the skills to carry out, and the awareness changes attitudes and behavior so that the personnel follow the prerogatives of the policies. Training must always be correlated with knowledge needs in order to fulfill a given task. If after the training, users do not follow a certain policy, it should be highlighted by awareness.

Ensuring business continuity

Any organization depends on resources, personnel and activities that are performed daily, in order to remain operational and profitable. Most organizations have tangible resources, intellectual property, employees, computers, communication links, buildings for main offices and workplaces. If any of these items are damaged or inaccessible for one reason or another, the company and the services provided by it may be severely affected. Depending on the severity of the cases, SC FILTRE AER CURAT S.R.L. can return to normal operating capacity faster or harder, but there are also situations in which companies are never able to resume their activity and maintain their customers following the various disasters that may occur. As a beneficial consequence of the implementation of the disaster recovery plan, it was found that organizations that have planned disaster recovery measures have a much higher chance of resuming their activity in time and remaining on the market.

Purpose of implementation by SC FILTRE AER CURAT S.R.L. of a disaster recovery plan is to minimize the effects of a disaster and to ensure that resources, personnel, and operations will resume their operation in a timely manner. A disaster recovery plan is implemented when a malfunction occurs, and all staff are concerned with restoring critical systems online again.

A Business Continuation Plan (BCP) has a broader approach to the problem. This includes the activation and operation of critical systems in another location while working on troubleshooting and restarting systems in the main location. It is also important to note that a company may be more vulnerable after a disaster, because the security services used for physical or logical protection may be unavailable or in a low capacity operating state. Availability is one of the main themes of continuity planning (disaster recovery plan and business continuation plan) in which it ensures that the necessary resources are in place to maintain the organization's operational under all conditions

When considering business continuity planning, some companies focus primarily on data backup and the existence of redundant hardware. Although these elements are extremely important, they are only small parts of the overall picture. Equipment needs people to configure and use it, and data is usually useless unless it is accessible to other systems and entities, possibly from the outside. Planning must take into account the presence of the right people at the right place, document the necessary configurations, establish alternative channels of communication (voice and data), the necessary power supply and ensure that all dependencies, including processes and applications, are properly understood and taken into account.

For example, where communication lines or a service is unavailable for any significant period of time, there must be a quick and tested way of re-establishing the affected communications and services.

Incidents and disruptions can occur for many reasons:

- Human - dissatisfied employees, riots, vandalism, accidents, theft, etc.;
- Technical- interruptions, viruses, worms, hackers, power supply problems, reliability of equipment, etc.;
- Natural - earthquakes, storms, fires, floods, etc.

Each of these situations can cause operating problems of the type:

- Minor - operations are unavailable for a short period of time, up to a few hours, or less than a day;
- Average - operations are unavailable for more than one day. In this case, a secondary location may be useful for further operations;
- Major - this type of event occurs after a disaster and the main location can no longer be used. An auxiliary location is required to continue operations until the main location is reactivated

The most important operations to be considered by the SC FILTRE AER CURAT S.R.L., in the normal functioning process are the following:

Data loss prevention and recovery capability

Within the daily operations of SC FILTRE AER CURAT S.R.L. it is very important to consider the security and protection of the processed data. Due to the fact that the security of the processed data is essential in any organization, preventing data loss and recovering it in the event of a disaster is critical. The main objective of a plan to save critical applications and data is to allow their restoration in a very short time and with minimal losses. The following points will be included in such a plan:

- Identifying the data and applications that need to be saved;
- The type of save for different data sets (full, partial, incremental, continuous backup); Regularity with which the backups will be made;
- Where backups will be kept;
- Who has access to the backups; ▫ The period of time needed to keep the data until it is destroyed.

The backups must be stored and access to them must be quick and easy. The location where security backups are stored can have a major impact on the process of restoring the affected data and services. For this reason, it is useful for security backups to be located in two different locations, so that the risk of losing them has been significantly reduced.

Ability to respond to incidents

When creating a disaster response plan, both the ability to respond to incidents and the identification of short-term and long-term objectives should be considered, as follows:

Identification of critical functions and priorities for restoration;

- Identification of the support systems necessary for the critical functions;
- Estimating the potential problems that may arise and identifying the minimum resources needed for disaster recovery;
- Choosing the recovery strategy and identifying the vital elements needed to resume the activity (personnel, equipment, systems, etc.);
- Identification of the person (s) who will lead the resumption of the activity and the process of testing
- Calculation of the funds needed to achieve these objectives.

The plan will also need to detail how to contact and mobilize employees, communicate between employees, interface with external suppliers.

Maintenance, monitoring and evaluation of audit logs

After completing the procedures for testing the disaster recovery plan, it is important that it is maintained, updated and continually evaluated. These activities consist of:

- Accountability of staff FILTRE AER CURAT S.R.L. - the job description of the persons responsible for the disaster recovery plan must contain details about their responsibilities within the disaster recovery plan;
- Performance review - carrying out (or failing to carry out) the actions of maintenance of the disaster recovery plan during white meetings with the responsible persons;
- Audit – the audit team must check the plan and ensure it is also updated according to reality.

At the same time, the audit team will have to inspect all the additional locations where the backup, security policies, configurations, etc. are stored.

Also, the implications of the disaster recovery plan for maintenance, monitoring and recovery should be considered by the SC FILTRE AER CURAT S.R.L. in any discussions regarding the purchase of new equipment, modification of existing ones or critical infrastructures of SC FILTRE AER CURAT S.R.L.

Penetration Tests

Security testing is an important element in the process of ensuring business continuity
S.C. FILTRE AER CURAT S.R.L. and consists of a comprehensive analysis of the behavior of the systems and applications of the organization under predetermined scenarios of computer attack.

The purpose of penetration tests is to analyze the behavior of applications in the context of different computer attacks, analyzing the vulnerabilities that may exist in the applications developed or used. A complete penetration test includes both automatic and manual tests. Automated tests identify negligence or programming errors in the applications used and are performed using specialized programs (vulnerability scanners, fuzzers, code scanners, etc.). Manual tests are used to analyze aspects of applications that require human intuition, identifying logical programming errors.

It is recommended that a penetration test (external and internal) to be performed annually by S.C. FILTRE AER CURAT S.R.L.

Penetration tests do not solve the problems of computer applications and systems, but only identify them. After each penetration test, actions to correct and update the systems and applications in the tests are required.

Periodic safety assessments and remedial arrangements

The world of computer security is constantly developing. There are a variety of attack and defense methods that can be used both to attack a computer system and to defend it. The assessment of information systems security shall be achieved by:

- Security Policy Review - Security policies are used to check the presence and rigor of the security controls implemented;

- Periodic scanning to identify computer vulnerabilities (vulnerability scanning) - these programs are used to detect the problems of computer applications, misconfigurations, and security vulnerabilities;
- The remediation of the security issues - is based on reports resulting from periodic security scanning tests. The remediation is done by implementing the security patches provided by the software manufacturers, updating the latest version of the applications, reconfiguring the targeted computer systems, etc.

Penetration tests - are mainly used to evaluate the remedial measures implemented following security scans.

Cyber-attacks and preventive measures

Romania is currently facing threats from the cyber space against critical infrastructures, given the increasing interdependence between cyber infrastructures and infrastructures such as those in the energy, telecommunications, transport, financial-banking, and national defense sectors.

The globalization of cyber space is likely to amplify the risks to them, affecting the private and public sectors alike. The threats specific to the cyber space are characterized by asymmetry and accentuated dynamics and global character, which makes them difficult to identify and counteract by measures proportional to the impact of the materialization of the risks. Threats to the cyber space can be classified in several ways, but the most commonly used ones are those based on motivational factors and the impact on society.

In this respect, we can consider cyber-crime, cyber-terrorism, and cyber war, with both state and non-state actors as its source.

Threats in the cyber space materialize - by exploiting vulnerabilities of a human, technical, and procedural nature - most often in:

- cyber-attacks against infrastructures that support public utility functions or information society services whose interruption/ damage could be a threat to national security;
- unauthorized access to cyber infrastructures;
- unauthorized modification, deletion or deterioration of computer data or illegal restriction of access to such data;

- cyber espionage;
- causing damage to property, harassment, and blackmail of natural and legal persons, in public and private law.

The dangers and threats in the virtual space generally concern the networks, the network nodes and the vital centers, more precisely, their physical equipment and systems (computers, supplies, connections and network nodes, etc.), as well as the other infrastructures that shelter them in this way. of means (buildings, electricity networks, cables, fiber optics and other components). To the same extent, they also target data centers, systems for storing, storing, and distributing information, material support of databases and much more.

But first and foremost, such dangers and threats concern IT systems (companies, production lines, supply systems with strategic materials, resource and market infrastructures, research institutes, communications systems).

The following are also included in the category of dangers and threats against critical infrastructures of cyber space:

- developing subversive and unconventional IT networks;
- the increasingly intense activity of hackers;
- Cyber terrorism.

Without an implemented and functional security system, computer, telecommunication systems and data processed, stored, or transported by them can be subjected to computer attacks at any time. Some attacks are passive - the information is monitored or copied, and other attacks are active - the flow of information is changed with the intention of corrupting or destroying data or even the system or network itself. IT and telecommunications systems, their networks and information in their possession are vulnerable to numerous types of attacks if they are not protected by an effective cybersecurity plan.

THE COMMITMENT OF THE COMPANY

The Company undertakes to implement measures to ensure the security of information to protect unauthorized leaks of personal data.

This policy must be respected by all employees of FILTRE AER CURAT S.R.L. and other third parties who have access to the personal data of the organization or interact in some way with the targeted individuals and/ or the information systems of the Company

CONSEQUENCES

Failure to comply with this Policy by the Company's employees may result in disciplinary sanctions (including termination of employment contract) and, depending on the circumstances, court action for full recovery of the damages brought as a result of non-compliance with this Policy.

Failure to comply with this Policy by business partners may lead to termination of commercial contracts and, depending on circumstances, court action for full recovery of damages brought to SC FILTRE AER CURAT S.R.L. as a result of non-compliance with this Policy.

SC FILTRE AER CURAT S.R.L. will communicate this Policy to all employees, collaborators, business partners or other third parties.

Policy approved by:	
Signature:	
The following review:	

Annex I

COMMUNICATION OF POLICY

I declare that I have read that I agree and that I agree to comply with this Policy

Name and Surname/ Company Name/ Position	**Signature**
Example #1 Ion Ionescu/ HR manager	
Example # 2 ABC SRL by Ion Ionescu, Director	
Name and Surname/ Company Name/ Position	**Signature**

Development of this Policy was possible thanks to ANSSI and the materials published on http://anssi.ro/