Infrastructure Security Policy

INDEX

1. EXECUTIVE SUMMARY

The Specific Information Security Policy for Infrastructures aims to complement the Information Security Policy of Altice Portugal, in order to regulate and implement good practices of security and information protection.

This Specific Policy for Infrastructures applies to all Systems and users of the internal network of Altice Portugal - ptNet. This document defines its attributions and regulates their operation, in order to guarantee the adequate levels of security and protection of the Information.
The Specific Information Security Policy for Infrastructures applies to the Infrastructure layer that supports the Information Technology[1] and Communications Infrastructures[2] of Altice Portugal.

2. SCOPE

This Policy is applicable to all employees, suppliers, and service providers, external entities that access the Information Technology, Information Systems, Networks and Service Platforms of Altice Portugal.

Within ptNet, the term "user" will be used as a reference to any of the individuals referred to above.

It is essential to ensure that all users, regardless of their hierarchical level, function and / or contractual linkage - internal to Altice Portugal or their companies in which they have an interest in external entities or others with whom Altice Portugal has contracted the supply of Products / Services - are aware of this policy and adequate access to the information necessary for the performance of their duties, requiring them to respect the implemented security controls and compliance with the integrity, confidentiality and availability of information.
All access to information, infrastructure or information systems owned by Altice Portugal by external collaborators or partners requires the pre-signing of a Non-Disclosure Agreement (NDA), even after the end of the provision of the service.

2.1 Exceptions to Policy

All requests for exceptions to Altice Portugal's Specific Information Security Policy for Infrastructures must be duly justified, authorized and documented. These requests should be sent to the Directorate of Cybersecurity.

2.2 Policy Review

The Specific Information Security Policy for Infrastructures is reviewed annually, or whenever warranted in terms of technical or business needs.

[1] Any combination of devices, network equipment, platforms, processes, applications, interactive or otherwise, fully or partially automated, which use, store, transport or transform information

[2] Systems, equipment and network elements that support the communications services provided by Altice Portugal

3. User Duties

The ptNet user universe consists of all the employees of the Altice Portugal group, outsourced outsourcers, as well as elements outside the company that require temporary access (eg suppliers, consultants and auditors). PtNet users have the following security responsibilities regarding security:

1. Take care of the equipment assigned to them, both in order to guarantee a use in the scope for which the equipment was allocated, as well as for their safety (and of the information contained therein) and operability;
2. Compliance with copyright law is strictly the responsibility of users. Is not allowed the use of peripheral equipment data storage, such as CD recorders, USB disks or similar to copy computer programs, multimedia data or any other document that refers property protection (copyright), under which copy is not permitted;
3. Ensure the confidentiality of the access credentials entrusted to them;
4. Ensure the company's information security, assigning the appropriate classification if owners of it, respecting the classification of the information to which they have access, proceeding accordingly to the handling rules, regarding to its confidentiality and integrity. If in the performance of their activities, if the users of ptNet came into the possession of confidential or proprietary information, they must ensure that are processed with the utmost confidentiality, not disclosing to third parties;
5. Safeguard documents (availability) related to the users professional activity, storing them in central servers, thus ensuring their protection through backup processes and information security in accordance with the information security protection level. Automatic Backup processes ensure availability for replacement of the information stored on central servers;
6. Delete user’s documents of central servers whose validity is exceeded or are no longer relevant to the user's work or the business of Altice. There are disk space quotas for information storage, assigned by Director or group. The shares may be changed on request, properly justified by the respective Direction;
7. Personal documents must be stored exclusively on the user's computer, in easily identifiable a space. The information size should be kept in a level that can’t jeopardize the performance of the equipment;
8. Users are responsible for not having risky behavior (handling of e-mail, malware, browsing dangerous websites, etc.) that endanger the systems or the company information. They also have to report situations or anomalies (suspicions) that may be related to the logical security of IT, SI or Altice Portugal network.

4. ARCHITECTURE

The Engineering and Network Management Department is responsible for:

- The Datacenter Network and Security infrastructure architecture;
- The WAN and LAN architecture definition and operational management.

The Engineering and Network Management Department is the entity authorized to make requests to internal suppliers regarding the network infrastructure or internal systems (eg. Telco systems / platforms), whether new implementations, installations, links, alterations, accesses, addresses or others. In case of computing infrastructure and information systems, the authorized entity is the IT Department.

5. DOCUMENT MANAGEMENT

For the purposes of Document Management, will be used a single repository of information located in IBPMS, which ensures the availability and control of access to the data contained therein, as pre-established security levels.
This repository must comply with a regular Backup policy (STANDARD Backup Policies) and users defined therein shall comply with User Password Policy in this document, in order to ensure the requirements availability, integrity and confidentiality. This repository should also ensure the logging of access to all documents contained therein and the versioning (version control).

6. ACCESS MANAGEMENT

The accesses contemplated in this specific Policy are:

• ptNet (Internal Network of Altice Portugal);

• Remote access to ptNET;

• Local access.

All access above must comply with the guidelines contained in the Information Security Policy, namely:

- Inactive access for 60 days (maximum) should be blocked;
- If technically possible and no impact on the traceability of users, when are inactive for 1 year (maximum) they should be removed;
- Access to Systems and Applications included in the Internal Control Manual should be subject to periodic review by those responsible for the accesses, in order to reassess the need to maintain them;
- It is mandatory to carry out a procedure that periodically reassesses the need to maintain privileged access, accounts with administration privileges in all technologies, systems and applications;

- Any anonymous access (e.g. guest) is prohibited;
- All accesses require the existence of a procedure to support access requests and their authorizations, clearly indicating who is responsible for accepting the requests, as well as for their cancellation.

6.1 PTNET access (Internal Network)

This information was considered only for internal publication within the Organization.

6.2 Remote Access

This information was considered only for internal publication within the Organization.

6.3 Local Access to Datacenter

Local Access is the access to systems, platforms or infrastructure inside the Datacenter. Local Accesses can be assigned to technical teams (employees and service providers in outsourcing regime) and to clients that own infrastructure housed in Altice Portugal Datacenters, in this specific case, local access of clients, the necessities depend on the contracted services and the access is restricted to their infrastructure and means of access to it.

Local (logical) access necessarily implies physical access permissions to the Datacenter in question, in accordance with the physical access policy and procedures.

Only local access to systems, platforms or infrastructures is allowed when duly justified, and approved.

There are the following variants regarding the approval of local access:

- Internal Employees of Altice Portugal or its affiliated companies - The guidelines described in chapter 6.3 Local accesses apply. These accesses are necessarily nominal;
- Service providers (external collaborators) - The guidelines described in chapter 6.3 Local accesses apply. These accesses can be assigned by service provider;
- Clients - Access is restricted to the infrastructure itself and the level of access must be contractually determined and discriminated against. In addition to the guidelines described in chapter 6.3 Local accesses, it is necessary to discriminate, justify and approve the customer, as specified in the respective contract.

6.4 Automatic Controls and Periodic Revaluation of Access

Automatic controls of blocking / elimination of unused accesses, and procedures for periodic reassessment of accesses shall be implemented G4.2.1_PO.0005 Directives for Request, Authorization Revision of Accesses.

7. AUTHENTICATION

All information systems, infrastructures, and applications that require user authentication must centrally authenticate to the top Active Directory (AD). New isolated password management structures are not acceptable, except in cases where, due to the contingencies of classification of information, they require higher security requirements, in particular the use of strong authentication mechanisms.

Only complementary authentication systems will be accepted in the following situations:

- When centralized authentication is not feasible due to technical issues;
- In cases of incompatibility of certain equipment.

All events corresponding to abnormal / suspect authentication patterns should be sent to the SOC correlation and event correlation platform.

8. SECURITY IN RELATION TO SUPPLIERS

The relationship with our suppliers is guided by the compliance with established guidelines that aim to protect Altice Portugal's information accessed by suppliers in the context of its collaboration with Altice Portugal, as well as to safeguard the integrity of the services provided by Altice Portugal. Thus, the management of suppliers should be guided by the following guidelines:

- Access to Information: the supplier undertakes to access Altice Portugal's information and any clarifications it needs regarding any matter of the consultation and negotiation, abstaining from any improper use thereof, respecting the principles established in the Information Security Policy;
- Design and integration of secure systems: The supplier undertakes to ensure that integration and development processes, within the scope of the products and services provided, respect the principles established in the Information Security Policy;
- The Information Security Policy is made available to suppliers involved in the selection processes for the acquisition of products and / or services at the time of issuing the Tender Document or other relevant information (e.g. RFI3, RFQ4) within the scope of the selection;
- Suppliers involved in a selection process for the acquisition of products and / or services, in which the supplier has access to sensitive information, will sign a Declaration committing themselves to the general conditions contained in the specifications that will include, among others, the aspects of Confidentiality and Data Protection;
- Whenever Altice Portugal's relationship with suppliers shows that there is a need for contractual support or a legally equivalent instrument, these will include the obligation to comply with the Information Security Policy, in particular with regard to the confidentiality of information and obligation to protection of personal data.

9. STANDARDS FOR DEVELOPMENT OF APPS

This information was considered only for internal publication within the Organization.

[3] Request for Information

[4] Request for Quotation

10. Logging Of Activties And or Access

To safeguard accounts of users and systems, becomes necessary, in situations of force majeure, to inspect and to monitor communication activities in the network or of activity in certain systems. Only the IT and the Cybersecurity Departaments may execute or delegate the execution of these operations.
Preferably, the logs should be submitted to a centralized repository under the management of each administration team. Total or part of this information should be sent to the correlation platform, which supports the Security Operations Center (SOC) activity in identifying and detecting security incidents (see Chapter 17).

10.1 Logging Requirements

The logs of activities and access should be as indelible as possible, must have a minimum of 30 days retention and include the following information:

- IP - Source and destination of connections (network identification)
- Use of services
- Date and time of access to the systems (login and logout)

Whenever possible, logs of activities and access should also contain:

- Systems changes
- User ID (username)

10.2 Access Logging

The accesses regulated in this Policy must comply with the following logging requirements:

- ptNet: centred logging;
- Remote access: centred logging;
- Local access: in the system itself replicated for a centred logging.

10.3 Platform logging, to ensure legal requirements

The retention deadlines for the different types of information must be strictly ensured, in accordance with the legislation to which Altice Portugal is bound. The administrators of the platforms (eg RADIUS Telepac, RADIUS Prime, e-mail platforms, SAPO portal, etc.) are responsible for their availability and integrity.
This section covers any platform that allows a user or customer Altice Portugal, Internet access with public IP address under responsibility of Altice Portugal - these accesses should be accounting, and the records are preserved during retention time required by law or described in Service Order (OS32010CAPTP).

11. Eventos de Segurança

Infrastructures have to generate inherent security events, and have events recorded, namely:

- Authentication (eg login / logout, invalid authentication attempts, user account lockout);

- Access Control (eg creation / removal of user accounts and access profiles, access to critical objects, elevation of privileges);
- System (eg change of settings, start / restart of services);
- Attacks (eg detection / blocking of security attacks);
- Network (eg status of communication channels, active connections).

The generated events must record the following information attributes:

- The date and time of the event;
- The IP address of the system that generated the event;
- The ports and protocols used;
- The IP address of the system affected by the event;
- The identity responsible for the event;
- The description of the event.

Security events must be retained for at least 1 year.

12. ANTIVÍRUS

The existence of viruses (and malware in general) in standard stations, and especially in servers, are attack vectors par excellence that endanger the security of information and systems. To prevent receiving e-mail containing malware, all e-mail messages from corporate e-mail platforms should be inspected by an automatic virus detection and removal system.

12.1 Centralized Management of Antivirus

Antivirus Software, as well as its signatures, will be updated automatically. However, given the constant development of new viruses associated with their rapid dissemination, the effectiveness of this type of detection can't always be guaranteed at 100%, which is why initiatives can be taken to combat particular threats that may pass through measures (eg sending / requesting urgent extradat or AV pattern, local cleaning of workstations or servers, etc.).

12.1.1 Standard Stations - Employee Environments

Standard Stations must contain anti-virus software installed, and users are required to allow (centralized) updating of the same.

12.1.2 IT Environment

The systems that support the technological infrastructure have, whenever they support it, to have installed a tool of detection and cleaning of virus. There will also be connectivity in the internal network that allows the communication of the centralized Antivirus platform with the systems.
Any system whose operation is compromised by the action of any malware should evaluate the possibility of being disconnected from the infrastructure to avoid further developments that reflect negatively on the same.

12.1.3 Client Environment (in Data Center)

Altice Portugal Datacenter client systems must have virus detection and cleaning tools. A centralized antivirus is recommended for client systems.
Any system whose operation is compromised by the action of any malware may be disconnected from the infrastructure to avoid further developments that reflect negatively on the same or the services provided.

In such cases, the customer must be advised by the respective manager of any changes or actions taken on their systems or of how it affects their service.

13. ANTI-SPAM

By definition, SPAM is considered to be any unsolicited, mass mailing for advertising purposes for malicious attacks called phishing when they are intended to capture information from the recipient.

- Anti-SPAM platforms allow you to mark SPAM e-mails that are received on e-mail platforms (in the inbound direction of the Internet for e-mail platforms) and can be delivered in a folder created for this purpose without causing any impact.

There are currently two anti-SPAM platforms covering the following universes:

- Corporate e-mail (Altice Portugal group domains)
- Customer domains Altice Portugal.

14. SOFTWARE UPDATES

In terms of impact, non-installation of security-related software updates allows one or more vulnerabilities, from the public domain, to be exploited to attack (eg malware) such systems.

14.1 Systems

The installation of patches is the responsibility of the Systems administrators of the respective platforms. Whenever there are technical impediments that support the non-installation of patches, situations should be considered exceptions, and be properly documented.
Updates should be formally planned, in accordance with current procedures, which should include the fall-back procedure.
In the case of customer systems, the updates require the prior agreement of the respective customer. Any system whose operation is compromised due to the non-installation of patches can be disconnected from the infrastructure to avoid further developments that reflect negatively on the same or on the services provided. In such cases, the customer must be advised by the respective manager of any changes or actions taken on their systems or of how it affects their service.

14.2 Workstations

The responsibility for distributing security patches to workstations is from the Desktop Management teams. The distribution of security updates performed within the scope of Desktop Management should guard against the impact on the network.
It is recommended to distribute updates outside of normal working hours or at the weekend, or even the phased distribution (by batch of workstations).

15. WATCH SYNCHRONIZATION

In order to ensure that all records that include timestamps (eg, logs, events to correlate, traffic data, etc.) refer to the same time frame, thus ensuring their legal validity, it is imperative that all systems are synchronized in clock terms by a single time frame.
Thus, all systems must synchronize their clocks with the centralized Network Time Protocol (NTP) platform. At the security level of the centralized NTP platform, it is recommended:

- NTP platform, it is recommended: The use of a suitable topology and with the sufficient number of clock sources that guarantee its availability;
- Where technically possible, the use of encryption that guarantees the authenticity and integrity of the clock information made available to the various systems.

16. SECURITY INCIDENTS

Generally, a security incident is an action or set of actions taken against a computer or computer network that results in, or may result, in an impairment of the basic properties of information security: availability, integrity and confidentiality.
In line with the incident management process, the specific designations should be used:

- Security incidents: this is defined as any breach or imminent threat of a breach of the Information Security Policy, of Acceptable Use Policies of services provided, or of good security practices adopted by the Organization. This definition covers any anomaly that affects or could affect information security, including its essential properties: confidentiality, availability and integrity.
- Information Security Event: is the record of any occurrence of observable cybersecurity in a system or network.

16.1 Incident Classification

Incident classification used is the one established by CERT.PT and adopted by the National CSIRTs, which Altice Portugal is a member through its CSIRT. This classification is based on the result obtained or intended by the attack. http://www.cert.rcts.pt/images/docs/Taxonomiav2.5.pdf

16.2 Security Incident Comunication

Whenever an anomalous situation is identified that may be related to the logical security of Altice Portugal's IT, SI or network (eg, knowledge of machines infected with malware, phishing emails affecting Altice Portugal or its image, theft of credentials, etc.), it should be immediately communicated to Altice Portugal's CSIRT **(csirt@telecom.pt)**
The contact should be made via email to CSIRT Altice Portugal or a ticket can be created in Onedesk, 2.7 Cibersecurity, which will forward it after identifying the respective interlocutor.
The information received is used in the treatment of the incident respecting the current laws of privacy and protection of personal data. The information of personal data is not released to third parties and, in case of real necessity, the expressing authorization is requested to the person / entity.

17.SECURITY OPERATIONS CENTER (SOC)

SOC is a centralized team at Altice Portugal, specialized in Information Systems Security, responsible for the detection and response to Security incidents.

The systems, platforms and technologies critical to the business of Altice Portugal, should be under the monitoring of the SOC.

In addition, events generated by technologies for detecting logical security vulnerabilities, intrusion detection systems, antivirus, firewalls, and centralized authentication platform should be sent to the SOC event monitoring and correlation platform.

18. Operating System Configuration Standard

The following general installation procedures should be followed for all system implementations:

1. If the machine is a new installation, it must be protected from hostile network traffic until the operating system is installed and hardened;
2. Operating system installation;
3. Upgrading all operating system software according to vendor recommendations;
4. Configure the operating system parameters according to CIS Benchmarks (OS hardening).

18.1 Windows Systems

The following installation and configuration procedures should be followed for all Windows based system deployments:

Step	Action	CIS Benchmark Reference
	Preparation and Installation	
1	If the machine is a new installation, it must be protected from hostile network traffic until the operating system is installed and *hardened*	
2	Consider using the Security Configuration Wizard to assist in hardening the host	
	Service Packs and Hotfixes	
3	Install the latest service packs and hotfixes from Microsoft	
4	Enable automatic notification of patch availability	
	User Account Policies	
5	Set minimum password length	1.1.4
6	Enable password complexity requirements	1.1.5
7	Do not store passwords using reversible encryption	1.1.6
8	Configure account lockout period	1.2
	User Rights assignment	
9	Restrict the ability to access this computer from the network to Administrators and Authenticated users	2.2.2
10	Do not grant any users the 'act as part of the operating system' right	2.2.3
11	Restrict local logon access to Administrators	2.2.6
12	Deny guest accounts the ability to logon as a service, a batch job, locally or via RDP.	2.2.18-21
	Security Settings	
13	Disallow users from creating and logging in with Microsoft Accounts	2.3.1.1
14	Disable the guest account (default)	2.3.1.2
15	Require Ctrl-Alt-Del for interactive logins (default)	2.3.7.2
16	Configure machine inactivity limit to protect idle interactive sessions	2.3.7.3
17	Configure MS Network Client to always digitally sign communications	2.3.8.1-2
18	Disable the sending of unencrypted passwords to third party SMB servers	2.3.8.3

19	Configure MS Network server to always digitally sign communications	2.3.9.2-3
	Network Access Controls	
20	Disable anonymous SID/Name translation (default)	2.3.11.1
21	Do not allow anonymous enumeration of SAM accounts and shares	2.3.11.2-3
22	Do not allow Everyone permissions to apply to anonymous users (default)	2.3.11.4
23	Do not allow any named pipes to be accessed anonymously.	2.3.11.5
24	Restrict anonymous access to named pipes and shares (default)	2.3.11.8
25	Do not allow any shares to be accessed anonymously	2.3.11.9
26	Require the "Classic" sharing and security model for local accounts (default)	2.3.11.10
	Network Security Settings	
27	Allow Local System to use computer identity for NTLM	2.3.12.1
28	Disable Local System NULL session fallback	2.3.12.2
29	Configure allowable encryption types for Kerberos	2.3.12.4
30	Do not store LAN Manager hash values	2.3.12.5
31	Set LAN Manager authentication level to only allow NTLMv2 and refuse LM and NTLM	2.3.12.7
32	Enable the Windows Firewall in all profiles (domain, private, public) (default)	9.[1-3].1
33	Configure the Windows Firewall in all profiles to block inbound traffic by default (default)	9.[1-3].2
	Active Directory Domain Member Security Settings **Active Directory Domain Controller Security Settings**	
34	Digitally encrypt or sign secure channel data (always) (default)	2.3.6.1
35	Digitally encrypt secure channel data (when possible) (default)	2.3.6.2
36	Digitally sign secure channel data (when possible) (default)	2.3.6.3
37	Require strong (Windows 2000 or later) session keys	2.3.6.6
38	Configure the number of previous logons to cache	2.3.7.6
	Audit Policy Settings	
39	Configure Account Logon audit policy	17.1
40	Configure Account Management audit policy	17.2
41	Configure Logon/Logoff audit policy	17.5
42	Configure Policy Change audit policy	17.7
43	Configure Privilege Use audit policy	17.8
	Event Log Settings	
44	Configure Event Log retention method and size	18.7.19
45	Configure log shipping for centralized logging (e.g. to Splunk)	
	Additional Security Protection	
46	Disable or uninstall unused services	
47	Disable or delete unused users	
48	Configure User Rights to be as secure as possible	
49	Ensure all volumes are using the NTFS file system	
50	Configure file system permissions	

51	Configure registry permissions	
52	Disallow remote registry access if not required	2.3.11.6
	Additional Steps	
53	Set the system date/time and configure it to synchronize against campus time servers	
54	Install and enable anti-virus software	
55	Install and enable anti-spyware software	
56	Configure anti-virus software to update daily	
57	Configure anti-spyware software to update daily	
58	Install software to check the integrity of critical operating system files	
59	If RDP is utilized, set RDP connection encryption level to high	
60	Install EMET	18.7.17
	Physical security	
61	Set a BIOS/firmware password to prevent alterations in system start up settings	
62	Disable automatic administrative logon to recovery console	2.3.13.1
63	Do not allow the system to be shut down without having to log on	2.3.14.1
64	Configure the device boot order to prevent unauthorized booting from alternate media	
65	Configure a screen-saver to lock the console's screen automatically if the host is left unattended	

Check the latest configuration guides with https://benchmarks.cisecurity.org/tools2.

18.2 Linux Systems

The following installation and configuration procedures should be followed for all Linux-based system deployments:

1. If the machine is a new installation, it must be protected from hostile network traffic until the operating system is installed and hardened;
2. Operating system installation;
3. Upgrading all operating system software according to vendor recommendations;
4. Configure the operating system parameters according to CIS Benchmarks (OS hardening) including:
    a. Disable all unused services;
    b. Disable unsafe services such as Telnet and FTP and install equivalent secure services (SSH, SFTP);
    c. Desativar logins remotos para root;
    d. Install GR Security;
    e. Configure log shipping for centralized logging (eg Splunk);
    f. Install a File Integrity Monitor or Host-IDS (e.g., OSSEC);
    g. Avoid performing services as root;
5. Physical security:
    a. Set a BIOS / firmware password to prevent changes to settings at system startup;
    b. Configure the device boot order to prevent unauthorized booting from alternative media;
    c. Configure the screen saver to automatically lock the screen when it is left unattended.

Check the latest configuration guides with https://benchmarks.cisecurity.org/tools2.