Data Center, Virtual Data Center and Data Protection Services

Security & Compliance Statement

Date: 06-10-2023

D_GP_001 Revision: 5.0

Index

1 Document Objective and Scope

This document defines the characteristics and procedures implemented in Ar Telecom services relative to security and compliance. The document focuses on confidentially, availability and integrity of customer data.
Its applicability is restricted to the following services:
Data Center Housing services: Client infrastructure installed in Ar Telecom's production data center in Lisbon, including:

- Physical housing of equipment
- Connectivity provided for the hosted equipment
- Electrical supply of the equipment
- Remote hands servicing of the equipment

Virtual Data Center services: Virtual machines provided to the customer, hosted in Ar Telecom's production datacenter in Lisbon or in the disaster recovery data center in Porto, including:

- Computing resources
- Storage resources
- Networking and connectivity of the virtual environments
- Firewall infrastructure
- Backup infrastructure
- Licensing services
- Managed services (backup, operating system administration, firewall and vpn administration
- Disaster recovery services

Data Protection Services: Backup & Disaster recovery solutions based on replication of customer data to the Ar Telecom Data Centers in Lisbon or Porto:

- Computing resources
- Storage resources
- Networking and connectivity of the virtual environments
- Firewall infrastructure
- Backup infrastructure
- Licensing services
- Managed services (backup, operating system administration, firewall and vpn administration.

This document is a summary of Ar Telecom's Business Continuity and Security Plan, that are confidential documents and thus cannot be shared with clients.

2 Information Security Checklist

2.1 High Level Checklist

These certifications and procedures are in place in the organization.

- **Scope of Information security arrangements**: There are established Information Security Management System in place in the organization. The organization complies and is certified by SGS on ISO27001 and by APCER on ISO20000. The scope of the ISO27001 included all services provided by the company and the scope of ISO20000 includes all services within the scope of this document (Data center, Virtual data center and Data protection services).
- **Personnel vetting and background verification of employees** is performed to the full extent allowed by Portuguese law.
- **Professional qualifications of information security staff**: Information security within the organization is carried out by an internal and external team that overall have the following certifications: CANS-Certified Auditor for the National Security Office; CIA–Certified Internal Auditor, CISA – Certified Information System Auditor; CFE–Certified Fraud Examiner; CISSP–Certified Information System Security Professional; PCI DSS QSA–Qualified Security Assessor; ISO 27001 Lead Auditors; ISO 20000 Master; ISO 27032 Lead Cybersecurity Manager.
- **Awareness and training**: There are mandatory Information Security awareness and training programmes provided for all employees on at least an annual basis. This program is audited in the scope of ISO27001.
- **Information classification**: There is documented guidance on information classification and it is reviewed on a regular basis. This documentation and review process is audited in the scope of ISO27001.
- **Access control and management**: There are access controls mechanisms, including separation of duties, logical and physical controls in place and monitored according to the data classification policy. These systems and processes are audited in the scope of ISO27001 and ISO20000.
- **Access management**: Accesses are granted, reviewed, revoked and validated on a role-based fashion. These systems and processes are audited in the scope of ISO27001 and ISO20000.
- **Data destruction and lifecycle management**: There is a data life cycle management and destruction policy and it is audited in the scope of ISO27001 and ISO20000.
- **Physical security**: The organization follows the best practices regarding physical security, namely using CCTV, multiple access system checkpoint, and physical security personnel. These system and processes are audited in the scope of ISO9001, ISO27001 and ISO20000.
- **Incident management**: The organization has an established process for notifying customers or acquirers upon discovery of an Information Security Incidents. These processes are audited in the scope of ISO27001 and ISO20000.
- **Risk management**: The organization performs periodic Information Risk Assessments of the business units, processes, applications, systems and facilities. Processes audited in the scope of ISO27001 and ISO20000. The results of Information Risk Assessments are monitored and recorded in a risk register.
- **Change management**: The is a Change Management Process in place that ensures that proposed changes to Customer Services, Business Applications, Computer Systems and Networks are authorized and tested prior to deployment. These processes are audited in the scope of ISO20000.
- **Business continuity**: The organization has a documented and tested Business Continuity Plan.
- **Disaster recovery**: The organization has documented and tested Disaster Recovery infrastructure and plans for its critical infrastructures and for customers that subscribe disaster recovery services.

2.2 Infrastructure as a Service Checklist

These certifications and procedures are in place in the organization.

- **Certification**: The hosting location is included in the scope and audited in compliance to ISO 9001, ISO 14001, ISO 27001 and ISO 20000.
- **Data handling**: There is a data classification policy in place and the organization provides employees with guidelines for handling customer data.
- **Encryption**: The organization provides infrastructure and services to encourage customers to encrypt data in transit and at rest according to industry best practices. For data transmission the organization provides MPLS, IPSEC, SSL or L2TP based encryption and for data storage the data at rest encryption is provided using native encryption from storage manufacturers.
- **Backup**: The organization has backup policies for its own services and provided backup services to customers. Data in transit among the IaaS platforms and backup systems is encrypted.
- **Credentials Management**: The organization has credential management processes that ensure tracking of access to the information and access on a need-only basis.
- **SLA Management**: The organization has a fully defined SLA policy that is visible to the customers. SLA's are defined for availability goals and for resolution times for incidents and requests.
- **Maintenance**: There are defined maintenance windows.

3 Physical Security

The following table lists the physical security controls implemented concerning the facilities used to house the equipment that provide the services in the scope of the document:

Ref.	Item	Controls, systems and procedures	Applicability
1.	Access control	1. Automated access control system with 3 checkpoints. 2. Logging of accesses. 3. 24x7 physical presence of at least two security personnel. 4. Access validation based on pre validated access lists.	All services 3. and 4. Not available on DR data center
2.	CCTV monitoring	1. 24x7 recording of exterior facilities 2. 24x7 personnel monitoring of exterior facilities 3. 24x7 recording of interior facilities 4. 24x7 personnel monitoring of interior facilities	All services 2. and 4. are not available on DR data center.
3.	Fire protection	1. Automatic detection 2. Automatic extinction: a. CO_2 extinction for electrical rooms b. Inert gas extinction for equipment rooms c. Foam extinction for diesel exposed areas	All services
4.	Flooding protection	1. Automatic detection of humidity in all technical areas. 2. Automatic water extraction through pumps. 3. Underground water pit barrier with automatic extraction.	All services 2. and 3. Not available at DR data center

4 Facilities Quality and Availability

The Housing Service provides accommodation at the Ar Telecom Data Center in Lisbon for companies wishing to host their own equipment on a high availability energy and internet connectivity infrastructure, with optimal security and climate conditions, namely:

- Building in reinforced concrete structure with floor 30 cm above the average ground level, lightning protection, technical rooms with fire compartment (for a minimum of 60 minutes), false floor and physically separated from the technical corridors up to 1 m in height by rows of concrete blocks, specific room for interconnection of operators, double ducts with distinct points of entry for physical connections to telecommunications networks and loading area and assembly with direct access to the exterior of the building.
- Privileged location in a low traffic density area, with easy access to Lisbon's main roads (CRIL, Axis N-S, A2 and A1) and with a public car park with a capacity of over 400 vehicles.
- High speed calls to major national and international destinations.
- Operation and maintenance team 24 hours / day x 7 days / week, consisting of specialists who always ensure the smooth operation and maintenance of the Center.
- Physical surveillance 24 hours / day x 7 days / week, performed in partnership with a duly certified private company, which ensures the correct compliance with the rules and security mechanisms in force.
- Video surveillance of internal areas and surrounding the Data Center.
- Access control through a centralized system, available 24 hours a day. Entrances and exits are recorded and all visitors are accompanied by members of Ar Telecom during their visits.
- Climatization through independent and actively redundant precision air handling units that guarantee a constant temperature in the Center of 21ºC +/- 2ºC with a relative humidity between 30% and 70%.
- Automatic fire detection and extinguishing based on a fire detection center that receives information from detectors spread throughout the building and controls the automatic extinguishing units by HFC23 (Data Center), by CO2 (PT, QGBT and generator set rooms) and by foam (generator set fuel tank room).
- Gas detection in support areas where there are batteries.
- Flood detection coupled with self-starting bilge pumps located in the drainage ditches in the technical corridors of the technical rooms.
- Power supply by two separate and autonomous circuits (for UPS operation), each based on a group of UPS, powered by the medium voltage utility ring, through its own sectioning and transforming station consisting of two dry transformers or by a generator set consisting of two redundant generators in the event of a public grid failure.
- ISO / IEC 27001 certification - systems and processes.

5 Business Continuity & DR

5.1 Introduction

Business continuity and disaster recovery are two different concepts. While Disaster recovery is the process of getting all important infrastructure and operations up and running following an outage. Business continuity differs in that it is the process of getting Ar Telecom's business back to full functionality after a crisis.
In this context DR specifically handles the recovery of infrastructures that are necessary to provide services for customers, BC handles the operationality of the organization after a crisis.

5.2 Business Continuity

Ar Telecom has a business continuity plan that comprises the processes and systems needed to ensure a sustainable operation in the event of an emergency:

- **Criteria**: The organization has a well defined process for determining the declaration of a technological or non-technological disaster.
- **Responsibility**: The BC plan clearly defines responsibilities for managing the operationalization of the plan.
- **Escalation**: The organization has appropriate escalation processes for BC activation.
- **Communication**: The BC plan defines how, when, whom and what should be communicated to clients upon plan activation.
- **Contact channels**: The BC comprises processes and systems to ensure the capability to communicate with clients.
- **Support processes**: The BC plan comprises processes and systems in order to ensure continued client support during an emergency.
- **Revenue assurance**: The BC plan includes systems and strategies that enable continued invoicing and collections from customers.

These plans, systems and processes are audited yearly by SGS (www.sgs.com) in the scope of the ISO 27001 certification process and by APCER (www.apcergroup.com) in the scope of the ISO 20000 certification process.

5.3 Disaster Recovery

Disaster recovery applies to Virtual Data Center services whenever the client as subscribed disaster recovery services and to network transmission and connectivity services that support all of Ar Telecom's operation.
The disaster recovery (DR) service for virtual machines hosted in Virtual Data Center ensures a replica of the contracted VMs in an alternative datacenter infrastructure located in Porto. DR service, in addition to VM replication, also ensures capacity reservation to start disaster services at the primary data center. The solution provides the following service levels:

- RPO (Recovery Point Objective): Maximum information replication delay, which may result in loss of information not yet replicated: 8 hours
- RTO (Recovery Time Objective): in the event of a disaster declaration or DR simulation, VMs will be activated in the alternate datacenter within: 48 hours

This service includes connectivity between Ar Telecom data centers, solution set-up including DR firewall configuration, and an annual activation or simulation.

Infrastructure rollback following a disaster statement (not applicable in case of a simulacrum) is performed by replicating the VMs to the production infrastructure. This action implies the deactivation of those, with a downtime not exceeding 24h. The rollback must be scheduled at least one week in advance.

Disaster Recovery infrastructure implies the following:

- Alteration of the public IP addressing
- No access to the management portal and hence the VMs console
- Firewall models may differ from production models. If the customer wishes to keep the same model, there may be additional costs. Depending on the model adopted in production, it may be mandatory to use the same model in the DR infrastructure.

6 Information Requests

The present document comprises the most often questions about Ar Telecom's services compliance with security and safety standards. To request further information about our services please use the following contacts:

Email: corporatebusiness@artelecom.pt

Please keep in mind that detailed information about Information Security, Data Protection and Business Continuity plans is sensitive data that Ar Telecom may not be able to share with customers.

For further information about the accredited auditors that certify our services use the following contacts:

INFORMATION SECURITY MANAGEMENT (ISO 27001)

www.sgs.com

Rua Cupertino Miranda, Pólo Tecnológico de Lisboa, Lote 6, Piso 0 e 1

Lisboa, 1600-513, Portugal

Phone: 808 200 747 / (+351) 229 994 500

INFORMATION SYSTEMS MANAGEMENT (ISO 20000)

www.apcergroup.com

Estrada do Paço do Lumiar - Campus do Lumiar, Edifício E, R/C

1649-038 Lisboa, Portugal

Phone: (+351) 213 616 430

info@apcer.pt