Aruba Cloud

Physical Security, Business Continuity and Disaster Recovery

CONTENTS

Aruba S.p.A.
Via San Clemente 53 - 24036 Ponte San Pietro (BG) – VAT no.: 01573850516
https://www.arubacloud.com - https://www.arubacloud.fr - https://www.arubacloud.es

1 HOUSING SYSTEMS AND CYBER SECURITY

In Italy, all the processing systems used for the delivery of the Aruba Group's Cloud services are located at the two data centers in Arezzo, "IT1" and "IT2", at Via Gobetti 96 and Via Ramelli 8 respectively, and the "IT3" data center in Ponte San Pietro (BG), at Via San Clemente 53.

Figure 1 – Data Center IT1

Figure 2 – Data Center IT2

Figure 3 – Data Center IT3

In addition to the Italian data centers, the Aruba Group has an international infrastructure network to deliver Cloud services, both proprietary and belonging to qualified partners, more specifically:

- CZ1 data center in Ktiš, in the Czech Republic, belonging to the international network of data centers owned by the Organization.
- FR1 data center, in Paris, France, belonging to the network of partner data centers.
- DE1 data center, in Frankfurt, Germany, belonging to the network of partner data centers.

- UK1 data center, in London, belonging to the network of partner data centers.
- PL1 data center, in Warsaw, Poland, belonging to the network of partner data centers.

Figure 4 – International Cloud Services Data Center Network

To meet rigorous quality standards, all data centers are ISO 9001 certified.

The next section explains the main physical security measures adopted.

1.1 Description of physical security measures

The data centers are ISO 27001 certified and boast all the main features required to guarantee physical security.

1.1.1 Tier 4*/Rating 4 and ISO 22237

The Aruba Group's IT1 and IT3 data centers comply with the highest level of the ANSI TIA 942-B-2017 standard (Rating 4). The A and B data centers within the IT3 campus also comply with ISO 22237, in terms of "Data center facilities and infrastructures", recognized as an international standard for the entire life cycle of the data center. This demonstrates the ability to avoid interruptions to services even in the event of serious faults (fault-tolerance), and was achieved thanks to a series of design and implementation measures covering all aspects of the data center: choice of site, architectural aspects, physical safety, fire-fighting systems, electrical system, mechanical system and data network.

A Rating 4 (formerly Tier 4) data center has redundant components constantly in operation, as well as multiple supply routes and hardware cooling systems.

The data centers are structured to withstand a fault in any part of the installation without causing downtime and are protected against physical events, also including natural catastrophes (e.g. fire, flood, earthquake, etc.).

1.1.2 Monitoring 24 hours a day

All data centers are monitored by a technical team 24 hours a day, 365 days a year.

The partner data centers are also managed remotely by the Aruba Group's technical team at the NOC (Network Operations Center).

In addition to the local control measures, the proprietary data centers have a BMS (Building Management System) capable of raising real-time alerts about significant events and allowing remote technicians to manage all the systems.

1.1.3 Physical access control

Access to the buildings is only possible for those who actually need it, by signing in at reception, and entry to the technical rooms is permitted only for authorized personnel, following identification with a pass and corresponding PIN.

For its proprietary data centers, the access control system includes the option to allow and disable individual swipe cards for specific areas, times and other criteria, guaranteeing complete security and ease of access.

At some partner data centers, such as FR1, DE1 and UK1, there is a biometric access control system in place.

1.1.4 Anti-intrusion systems

At all the data centers, grilles, bulletproof glass, armoured doors and motorized gates (passive anti-intrusion systems) are deployed, CCTV and VMD systems (active anti-intrusion systems) are installed.

In addition, motion sensors are installed at all areas of the data centers, capable of detecting the presence of people; in sensitive areas (data rooms, Power Centers, warehouses) there are also sensors that detect the opening of doors.

1.1.5 Fire-fighting, anti-flooding and anti-seismic building system

The data centers all respond to anti-seismic regulations. In addition, there are automatic fire detection and inert gas extinguishing systems, which are harmless to humans and IT systems, as well as flood detection systems.

Fire detection sensors are present on all floors of the buildings, as well as sensors that detect liquid leaks.

The buildings are also located in flat areas and in positions that have been surveyed with respect to ground level.

1.1.6 Redundant air-conditioning systems

The air-conditioning system for the data rooms and technological systems is made up of multiple redundant modules to ensure that it remains operational even in the event of multiple simultaneous failures.

The air conditioning system is protected by UPSs with batteries and emergency electricity generators in order to guarantee continuity of service.

1.1.7 Power supply and Power Center redundancy

The Aruba Group only uses servers and equipment with a dual power supply. For the output from every single Power Center there are STS (Static Transfer Switch) devices capable of guaranteeing continuity of power supply for both lines present, also ensuring that servers and equipment that do not have dual power supply continue working.

The power supply for the servers is completely redundant thanks to two separate Power Centers. Each Power Center has the capacity to supply all the data rooms in the proprietary data centers, even at full load, and is equipped with double conversion UPS systems with extremely high energy efficiency (2N + 1 redundancy for IT1, IT2 and IT3 and 2N for CZ1).

The power supply systems at the partner data centers are also completely redundant and equipped with double conversion UPS systems.

For more details on the technical characteristics of the data centers under analysis, please see the webpage: "Our data centers".

2 BUSINESS CONTINUITY AND DISASTER RECOVERY

2.1 Introduction

The objective of this chapter is to describe the Disaster Recovery and Business Continuity procedure in place to ensure its implementation in relation to Aruba Group Cloud services.

The business of all companies and their associated activities are heavily dependent on the availability of facilities and resources dedicated to supporting processes. In general, the impact of a service being unavailable increases as the interruption continues exponentially, and in a short time it is possible that the company's ability to operate is permanently compromised.

To ensure the continuity of Business Processes, it is extremely important to protect all the resources that contribute to the provision of the most critical services: information, people and infrastructure, technologies, communication networks, etc.

The Aruba Group has decided to implement a Business Continuity management program to analyze and manage the impact of certain disaster scenarios on operations and consequently identify recovery solutions to support business continuity.

These solutions address the restoration of essential services from an organizational, logistical and IT perspective.

2.2 Business Continuity Plan

The Business Continuity Plan (hereinafter referred to as "BCP" for the sake of brevity) is a set of rules and procedures that – by anticipating one or more scenarios that might interrupt the normal operation of any organized system – defines

the responsibilities, establishes the activities and provides the tools to manage the interruption and return the system to a sufficient state of operation.

The purpose of the BCP is to make sure that critical processes are restored within tolerable and preestablished deadlines.

The entire production environment related to Cloud services is protected by the company BCP, with Business Continuity tests on the infrastructure scheduled on an annual basis.

This role of this Plan is to provide guidelines for the Aruba Group when it comes to managing and moderate any risks identified by applying the "Information Security Risk Management" methodology, described in detail in the relevant chapter.

The BCP also defines and lists the measures to be taken before, during and after an emergency to ensure service continuity. It provides recommendations and, where possible, step-by-step instructions to guarantee the continuity of the Aruba Group's critical services in cases of undesirable events which may interrupt IT systems for any length of time.

2.3 Disaster Recovery

The Cloud environment consists of a multi-datacenter infrastructure, whose services are interconnected by a high-bandwidth, secure IPSEC network.

Each data center provides numerous types of services, including:

- Cloud Computing;
- Cloud Object Storage;
- Cloud Monitoring;
- Cloud Load Balancing;
- Private Cloud;
- Cloud Backup.

Each data center also has a structure made up of the following basic machines:

- Domain Controller;
- LVS Balancer;
- Front-End;
- WCF (Microsoft Webservice);

- Provisioning;
- Accounting and billing;
- Database;
- Hypervisor hosts;
- Cloud Storage hosts;
- Cloud Monitoring hosts;
- Private Cloud hosts;
- Cloud backup hosts.

Designed as a multi-data center structure, it is natively predisposed to Disaster Recovery, as all data centers are logically independent from each other.

It is important to highlight the fact that virtualized customer machines are not subject to geographical Disaster Recovery, as the customers themselves are provided with all the necessary tools to build tailor-made Disaster Recovery systems and procedures.