Aruba Cloud

# Bezpieczeństwo Fizyczne, Ciągłość Biznesowa i Disaster Recovery

14.04.2023

# SPIS TREŚCI





**AlphaNet Spółka z o.o.**
ul. Małobądzka 4a, 41-214 Sosnowiec
NIP: 644-318-61-65
https://www.arubacloud.pl

# 1 SYSTEMY HOUSING I CYBERBEZPIECZEŃSTWO

Trzy systemy przetwarzania, wykorzystywane do świadczenia usług Cloud Grupy Aruba, znajdują się we Włoszech, a dokładniej w data center „IT1" (Via Gobetti 96 w Arezzo), „IT2", (Via Ramelli 8 w Arezzo), w data center „IT3 DCA" oraz „DCB" (Via San Clemente 53 w Ponte San Pietro).

*Rys. 1 – Data Center IT1*

*Rys. 2 – Data Center IT2*

*Rys. 3 – Kampus IT3*

Oprócz włoskich data center Grupa Aruba dysponuje międzynarodową siecią infrastruktury do dostarczania usług w chmurze zarówno własnej, jak i należącej do wykwalifikowanych partnerów, a konkretnie:

- Data center CZ1 w Ktiš, w Czechach, będące częścią międzynarodowej sieci data centers należących do Organizacji.
- Data center FR1 w Paryżu, we Francji, należące do sieci data centers partnerów.
- Data center DE1 we Frankfurcie, w Niemczech, należące do sieci data centers partnerów.



**AlphaNet Spółka z o.o.**
ul. Małobądzka 4a, 41-214 Sosnowiec
NIP: 644-318-61-65
https://www.arubacloud.pl

- Data center UK1 w Londynie, w Wielkiej Brytanii, należące do sieci data centers partnerów.
- Data center PL1 w Warszawie, w Polsce, należące do sieci data centers partnerów.


*Rys. 4 – międzynarodowa sieć Data Center usług w chmurze*

Aby spełnić rygorystyczne standardy jakości, wszystkie data centers posiadają certyfikat ISO 9001.

W następnej części wyjaśniono główne środki bezpieczeństwa fizycznego, które zostały przyjęte.

## 1.1 Opis środków bezpieczeństwa fizycznego

Data centers posiadają certyfikat ISO 27001 i wszystkie główne cechy wymagane do zagwarantowania bezpieczeństwa fizycznego.

### 1.1.1 Tier 4* / Rating 4 i ISO 22237

Data center IT1 i IT3 Grupy Aruba spełniają najwyższy poziom normy ANSI TIA 942-B-2017 (Rating 4). Świadczy to o zdolności do unikania przerw w świadczeniu usług nawet w przypadku poważnych usterek ( tzw. tolerancja na awarie – ang. fault-tolerance) i zostało osiągnięte dzięki szeregowi działań projektowych i wdrożeniowych obejmujących wszystkie aspekty data center: wybór miejsca, aspekty architektoniczne, bezpieczeństwo fizyczne, instalację przeciwpożarową, instalację elektryczną, system mechaniczny i sieć danych.



**AlphaNet Spółka z o.o.**
ul. Małobądzka 4a, 41-214 Sosnowiec
NIP: 644-318-61-65
https://www.arubacloud.pl

Data center spełniające wymogi kategorii Rating 4 (dawniej Tier 4) ma stale działające redundantne komponenty, a także wiele sposobów zasilania i sprzętowe systemy chłodzenia.

Data centers mają taką strukturę, aby wytrzymać awarię w dowolnej części instalacji bez powodowania przestojów i są zabezpieczone przed zdarzeniami fizycznymi, obejmującymi również katastrofy naturalne (takie jak pożar, powódź, trzęsienie ziemi itp.).

### 1.1.2 ISO/IEC 22237

Data centers IT3 DCA i DCB Grupy Aruba posiadają certyfikację ISO/IEC 22237, zgodność z międzynarodowym standardem dla data centers przez cały cykl ich życia, od koncepcji strategicznej po budowę i eksploatację, zgodnie z ANSI/TIA 942 (standard amerykański) i EN 50600 (standard europejski). Regulacja zwana „Obiekty i infrastruktura data centers" obejmuje siedem obszarów: Koncepcje ogólne, Konstrukcję budowlaną, Dystrybucję energii, Kontrolę środowiska, Infrastrukturę okablowania telekomunikacyjnego, Systemy bezpieczeństwa oraz Informacje zarządcze i operacyjne.

### 1.1.3 Monitorowanie 24 godziny na dobę

Wszystkie data centers są monitorowane przez zespół techniczny przez całą dobę, 365 dni w roku.

Data centers partnerów są również zarządzane zdalnie przez zespół techniczny Grupy Aruba w NOC (centrum operacji sieciowych – ang. Network Operations Center).

Oprócz lokalnych środków kontroli własne data centers są wyposażone w system BMS (system zarządzania budynkiem - ang. Building Management System), który jest w stanie w czasie rzeczywistym alarmować o istotnych zdarzeniach i umożliwia technikom pracującym zdalnie zarządzanie wszystkimi systemami.



### 1.1.4 Kontrola dostępu fizycznego

Dostęp do budynków jest możliwy tylko w przypadku osób, które rzeczywiście go potrzebują, poprzez zgłoszenie się w recepcji, a wejście do pomieszczeń technicznych jest dozwolone tylko dla upoważnionego personelu, po identyfikacji za pomocą przepustki i odpowiedniego kodu PIN.

W przypadku własnych data centers system kontroli dostępu obejmuje opcję dopuszczenia i wyłączenia indywidualnych kart magnetycznych do określonych obszarów, godzin i innych kryteriów, gwarantując pełne bezpieczeństwo i łatwość dostępu.

W niektórych data centers partnerów, takich jak FR1, DE1 i UK1, funkcjonuje biometryczny system kontroli dostępu.

### 1.1.5 Systemy antywłamaniowe

We wszystkich data centers zastosowano kraty, szyby kuloodporne, drzwi pancerne i bramy automatyczne (pasywne systemy antywłamaniowe), zainstalowano systemy telewizji przemysłowej i systemy wizyjnej detekcji ruchu (aktywne systemy antywłamaniowe).

Ponadto we wszystkich obszarach data centers zainstalowane są czujniki ruchu, zdolne do wykrywania obecności osób; w obszarach wrażliwych (pomieszczenia z danymi, centra zasilania, magazyny) znajdują się również czujniki wykrywające otwarcie drzwi.

### 1.1.6 Instalacja przeciwpożarowa, przeciwpowodziowa i zabezpieczająca przed ruchami sejsmicznymi

Wszystkie data centers odpowiadają przepisom dotyczącym ochrony antysejsmicznej. Do tego dochodzą instalacje automatycznego wykrywania pożaru i gaszenia gazem obojętnym, nieszkodliwym dla ludzi i systemów informatycznych, a także systemy wykrywania zalania.

Na wszystkich piętrach budynków obecne są czujniki wykrywania pożaru, a także czujniki wykrywające wycieki cieczy.

Budynki znajdują się ponadto na terenach płaskich i w położeniu, które zostało zmierzone względem poziomu gruntu.

### 1.1.7 Redundantne systemy klimatyzacji

System klimatyzacji pomieszczeń danych i systemów technologicznych składa się z wielu redundantnych modułów, aby zapewnić jego działanie nawet w przypadku wielu jednoczesnych awarii.

System klimatyzacji jest zabezpieczony przez zasilacze UPS z akumulatorami oraz awaryjne generatory energii elektrycznej w celu zagwarantowania ciągłości działania.

### 1.1.8 Zasilanie i redundancja centrum zasilania

Grupa Aruba korzysta wyłącznie z serwerów i sprzętu z podwójnym zasilaniem. Na wyjściu z każdego centrum zasilania znajdują się statyczne przełączniki (STS), które są w stanie zagwarantować ciągłość zasilania dla obu obecnych linii, zapewniając również ciągłość pracy serwerów i urządzeń, które nie posiadają podwójnego zasilania.

Zasilanie serwerów jest całkowicie redundantne dzięki dwóm oddzielnym centrom zasilania. Każde z centrów zasilania ma zdolność zasilania wszystkich pomieszczeń danych we własnych data centers, nawet przy pełnym obciążeniu, i jest wyposażone w systemy UPS z podwójną konwersją o wyjątkowo wysokiej sprawności energetycznej (redundancja wynosząca 2N + 1 w przypadku IT1, IT2 i IT3 oraz 2N w przypadku CZ1).

Systemy zasilania w data centers partnerów są również całkowicie redundantne i wyposażone w systemy UPS z podwójną konwersją.

Więcej szczegółów na temat charakterystyki technicznej analizowanych data centers można znaleźć na stronie internetowej: „Nasze data centers”.



**AlphaNet Spółka z o.o.**
ul. Małobądzka 4a, 41-214 Sosnowiec
NIP: 644-318-61-65
https://www.arubacloud.pl

# 2 CIĄGŁOŚĆ BIZNESOWA I DISASTER RECOVERY

## 2.1 Wstęp

Celem tego rozdziału jest opisanie obowiązującej procedury Disaster Recovery i Ciągłości Biznesowej w celu zapewnienia jej wdrożenia w odniesieniu do usług cloud Grupy Aruba.

Działalność wszystkich firm i związane z nią działania są w dużym stopniu uzależnione od dostępności zaplecza i zasobów przeznaczonych do wspierania procesów. Ogólnie rzecz biorąc, wpływ niedostępności usługi wzrasta wraz z wydłużaniem się przerwy w sposób wykładniczy i w krótkim czasie może to doprowadzić do trwałego zagrożenia zdolności firmy do działania.

Dla zapewnienia ciągłości procesów biznesowych niezwykle ważna jest ochrona wszystkich zasobów, które przyczyniają się do świadczenia najbardziej krytycznych usług: informacji, osób i infrastruktury, technologii, sieci komunikacyjnych itp.

Grupa Aruba podjęła decyzję o wdrożeniu programu zarządzania Ciągłością Biznesową, którego celem jest analiza wpływu określonych scenariuszy awarii na operacje i zarządzanie nimi, a w konsekwencji identyfikacja rozwiązań naprawczych wspierających Ciągłość Biznesową.

Rozwiązania te dotyczą przywrócenia podstawowych usług z perspektywy organizacyjnej, logistycznej i informatycznej.



## 2.2 Plan Ciągłości Biznesowej

Plan Ciągłości Biznesowej (zwany dalej dla zwięzłości „PCB") jest zbiorem zasad i procedur, które – przewidując jeden lub więcej scenariuszy mogących przerwać normalne działanie dowolnego zorganizowanego systemu – określają obowiązki, ustanawiają działania i zapewniają narzędzia do zarządzania przerwą w działaniu i przywrócenia systemu do wystarczającego stanu działania.

Celem PCB jest zapewnienie, że krytyczne procesy zostaną przywrócone w akceptowalnych i wcześniej ustalonych terminach.

Całe środowisko produkcyjne związane z usługami w chmurze jest chronione przez firmowy PCB, przy czym testy Ciągłości Biznesowej infrastruktury są zaplanowane w cyklu rocznym.

Rolą niniejszego planu jest dostarczenie wytycznych dla Grupy Aruba w zakresie zarządzania i moderowania wszelkich ryzyk zidentyfikowanych poprzez zastosowanie metodologii „Zarządzania Ryzykiem Bezpieczeństwa Informacji", opisanej szczegółowo w odpowiednim rozdziale.

PCB również definiuje i wymienia środki, które należy podjąć przed, w trakcie i po wystąpieniu sytuacji awaryjnej, aby zapewnić ciągłość świadczenia usług. Zawiera zalecenia i tam gdzie to możliwe, instrukcje krok po kroku, które mają zagwarantować ciągłość krytycznych usług Grupy Aruba w przypadku niepożądanych zdarzeń, które mogą przerwać działanie systemów IT na dowolnie długi czas.

## 2.3 Disaster Recovery

Środowisko chmury składa się z infrastruktury wielu data centers, których usługi połączone są ze sobą bezpieczną siecią IPSEC o wysokiej przepustowości.

Każde data center oferuje wiele rodzajów usług, w tym:

- Cloud Computing
- Database as a Service
- Virtual Private Cloud – VPC
- Cloud Object Storage
- Domain Center
- Cloud Monitoring
- Cloud Backup

Każde data center ma również strukturę składającą się z następujących podstawowych maszyn:

- 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



**AlphaNet Spółka z o.o.**
ul. Małobądzka 4a, 41-214 Sosnowiec
NIP: 644-318-61-65
https://www.arubacloud.pl

- Cloud backup hosts

Zaprojektowane jako struktura z wieloma data centers, jest naturalnie predysponowane do obsługi Disaster Recovery, ponieważ wszystkie data centers są od siebie logicznie niezależne.

Należy podkreślić fakt, że zwirtualizowane maszyny klientów nie podlegają geograficznemu Disaster Recovery, ponieważ sami klienci otrzymują wszystkie niezbędne narzędzia do utworzenia dostosowanych do potrzeb systemów i procedur Disaster Recovery.



**AlphaNet Spółka z o.o.**
ul. Małobądzka 4a, 41-214 Sosnowiec
NIP: 644-318-61-65
https://www.arubacloud.pl

## HISTORIA WERSJI

| | |
|---|---|
| **WERSJA 1.1**<br>Z DNIA 14/04/2023 | ***CHARAKTER ZMIAN: Dodano: Certyfikacja ISO/IEC 22237 i Kampus IT3 w odniesieniu do DCA oraz DCB; zaktualizowano listę usług Cloud.*** |
| **WERSJA 1.0**<br>Z DNIA 01/01/2022 | ***CHARAKTER ZMIAN: Wydanie pierwsze*** |



**AlphaNet Spółka z o.o.**
ul. Małobądzka 4a, 41-214 Sosnowiec
NIP: 644-318-61-65
https://www.arubacloud.pl