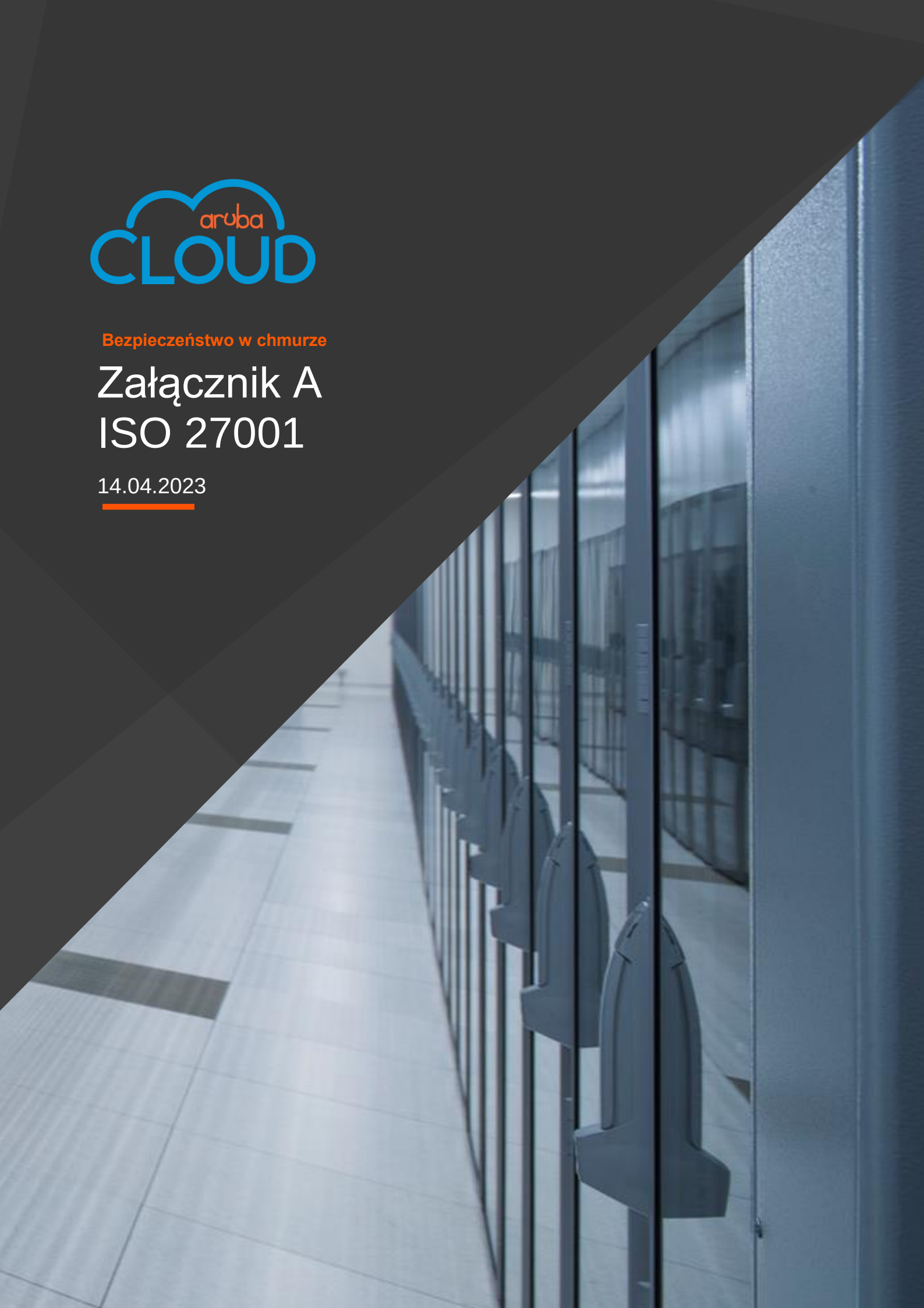
Bezpieczeństwo w chmurze

Załącznik A ISO 27001

14.04.2023



Załącznik A - ISO 27001 Aspekty bezpieczeństwa w chmurze Grupy Aruba			
Obszar kontroli		**Nasze kontrole**	**Narzędzia i funkcje dostępne dla Klienta**
A.5	**Polityka bezpieczeństwa informacji**	**Polityka systemu zarządzania bezpieczeństwem informacji (ISMS – ang. Information Security Management System)** - Grupa Aruba zdefiniowała przyjęte przez organizację podejście do zarządzania celami bezpieczeństwa informacji w określonej Polityce firmy. Niniejszy dokument został zatwierdzony przez Zarząd i opublikowany w firmowym intranecie. Dla wsparcia wyżej wymienionej Polityki opracowano dodatkowe zasady i procedury dotyczące konkretnych kwestii definiujących System zarządzania bezpieczeństwem informacji Grupy Aruba.	
A.6	**Organizacja bezpieczeństwa informacji**	**Role i obowiązki** - W ramach swoich obowiązków jako dostawcy usług w chmurze, określonych na stronie poświęconej modelowi współodpowiedzialności, Grupa Aruba określiła personel, role, umiejętności i obowiązki związane z procesami, zgodnie z zasadami segregacji obowiązków, możliwie najmniejszego poziomu dostępu i podwójnej kontroli. **Segregacja obowiązków (SoD – ang. Segregation of Duties)** - W ramach procesów operacyjnych Usług różne osoby odpowiadają za różne procedury, tak aby żadna z nich nie miała kontroli nad całym procesem. **Uprawnienia** - dostępu do pomieszczeń, urządzeń, danych, funkcji itp. są przyznawane pracownikom przypisanym do usług, zgodnie z zasadą „least privilege", tj. w zakresie niezbędnym do wykonywania przez te zasoby powierzonych im zadań, ale nie więcej. **Podwójna kontrola** - najbardziej krytyczne procedury z punktu widzenia bezpieczeństwa zakładają udział co najmniej dwóch osób.	**Role i obowiązki** - Ogólny opis usługi można znaleźć w Bazie wiedzy (KB), na stronie poświęconej ogólnemu opisowi usługi, wraz z tabelą lokalizacji usług i tabelą przedstawiającą model odpowiedzialności dzielonej między Grupę Aruba jako Dostawcę usług w chmurze i jej klientów.
A.7	**Bezpieczeństwo kadrowe**	**Szkolenie personelu** - personel serwisowy posiada odpowiednie umiejętności i doświadczenie oraz jest przeszkolony w zakresie każdej istotnej aktualizacji systemu. **Świadomość** - W ramach specjalnych szkoleń, okresowo pracownicy zapoznają się z kwestiami bezpieczeństwa, z ogólnym zarysem cyberprzestępczości i najlepszymi praktykami, które należy przyjąć. **Umowa o zachowaniu poufności (NDA – ang. Non Disclosure Agreement)** - Nowo zatrudnieni	**Szkolenie i świadomość** – Grupa Aruba udostępnia Bazę wiedzy zawierającą informacje na temat usług w chmurze. Zawiera ona informacje dotyczące usług, przewodniki, samouczki, dokumentacje dotyczące interfejsów programowania aplikacji (API), glosariusz i dziennik zmian usług.

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

Załącznik A - ISO 27001 Aspekty bezpieczeństwa w chmurze Grupy Aruba			
Obszar kontroli		**Nasze kontrole**	**Narzędzia i funkcje dostępne dla Klienta**
		pracownicy są zobowiązani do podpisania umowy o zachowaniu poufności w celu ochrony know-how firmy i innych poufnych informacji.	
A.8	**Zarządzanie zasobami**	**Spis inwentaryzacji zasobów** - Prowadzony jest zaktualizowany spis inwentaryzacji zasobów, który obejmuje rejestry wirtualnych i fizycznych urządzeń służących świadczeniu usług oraz ich fizyczną lokalizację w infrastrukturze Grupy Aruba. Spis inwentaryzacji zasobów jest aktualizowany po każdej instalacji w infrastrukturze nowego urządzenia. Ponadto, aby sprawdzić wszelkie rozbieżności, codziennie przeprowadza się automatyczne skanowanie sieci w celu wykrycia nowych zasobów. Spis inwentaryzacji zawiera opis zasobów, w których opisano stosowne cechy: na przykład rodzaj urządzenia (wirtualne lub fizyczne), infrastruktura, do której należy, wewnętrzna własność itp. **Zarządzanie zasobami** - Istnieją również wewnętrzne procedury, które definiują i formalizują działania związane z przygotowaniem nowych urządzeń i zarządzaniem nimi (np. sposób dokonania zmiany, aktualizowania systemów itp.). **Zarządzanie konfiguracją** - Lista komponentów systemu jest zdefiniowana tak, aby umożliwić identyfikację poszczególnych komponentów sprzętu i oprogramowania oraz ich modelu lub wersji. **Konserwacja i wsparcie** - Najważniejsze dla ciągłości Usługi komponenty sprzętowe (HW) są objęte umowami serwisowymi gwarantującymi naprawę lub wymianę w wystarczająco szybkim czasie przez dostawcę lub dostępność identycznych zmagazynowanych komponentów, które mogą zostać wdrożone w miarę potrzeb. Jeśli chodzi o oprogramowanie komercyjne (SW) istnieją odpowiednie umowy wsparcia, które gwarantują wsparcie techniczne dostawcy w przypadku nieprawidłowego działania. **Utylizacja** - Grupa Aruba gwarantuje, że przyjęto specjalne procedury dotyczące usuwania i niszczenia komponentów sprzętowych, które nie pozostają już w eksploatacji zarówno w kolokacyjnych zagranicznych centrach danych, jak i we własnych centrach danych, w celu zapewnienia,	**Własność zasobów** - zgodnie z zasadą współdzielonej odpowiedzialności, dla każdej usługi Grupa Aruba określiła odpowiednie atrybuty własności w odniesieniu do infrastruktury, licencji, adresów IP, oprogramowania dostarczonego przez Grupę Aruba, innego oprogramowania, danych i treści wprowadzonych przez klienta. Informacje o własności zasobów służących świadczeniu usług są dostępne dla klientów w publicznej bazie danych KB na dedykowanej stronie. **Usuwanie danych** - Korzystając z techniki czyszczenia dysku w środowisku chmurowym, w przypadku usług VPS (Smart), PRO i Private Cloud, klient ma możliwość trwałego usunięcia danych zawartych na swoim sprzęcie i uniemożliwienia ich odzyskania. Dedykowana strona Bazy wiedzy określa kroki operacyjne. **Oznakowanie** - Usługi Grupy Aruba umożliwiają klientom nazywanie i klasyfikowanie zasobów znajdujących się pod ich kontrolą. Przewodniki opublikowane w Bazie wiedzy zawierają dokładne instrukcje dotyczące wykonywania tych operacji i obowiązujące ograniczenia.

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

Załącznik A - ISO 27001 Aspekty bezpieczeństwa w chmurze Grupy Aruba			
Obszar kontroli		**Nasze kontrole**	**Narzędzia i funkcje dostępne dla Klienta**
		że dla każdego komponentu pamięci masowej, który osiągnął koniec jego żywotności i wymaga wymiany i utylizacji, dane w nim zawarte zostaną całkowicie i trwale usunięte.	
A.9	**Kontrola dostępu**	**Logiczne zarządzanie dostępem** - Przed uzyskaniem dostępu do systemów wewnętrznych upoważnieni pracownicy zostaną poproszeni o identyfikację i uwierzytelnienie się (za pomocą nazwy użytkownika, hasła i/lub karty elektronicznej). Po uwierzytelnieniu, pracownicy Grupy Aruba mogą uzyskać dostęp tylko do zasobów (np. systemów, danych), do których zostali wyraźnie upoważnieni, zgodnie z rzeczywistymi potrzebami właściwymi dla zajmowanego stanowiska. Użytkownicy są zarządzani za pomocą kontrolerów domeny usługi Active Directory (AD). Aby zagwarantować zasadę „segregacji obowiązków", logiczny dostęp do środowiska produkcyjnego jest zarządzany przez AD w dedykowanej domenie, w której znajdują się użytkownicy o różnych przywilejach i uprawnieniach zgodnych z zawodową rolą danej osoby i zgodnie z zasadą możliwie najmniejszego poziomu dostępu. Wszyscy użytkownicy są identyfikowanymi osobami, więc nie ma użytkowników grupowych i/lub współdzielonych i są oni okresowo poddawani niezależnej weryfikacji przez Dział Bezpieczeństwa. **Polityka haseł** - Zgodnie z polityką bezpieczeństwa grupy i zgodnie z przepisami dotyczącymi prywatności („środki minimalne", przepisy Urzędu Ochrony Danych), stosuje się bezpieczną politykę zarządzania hasłami. Po utworzeniu użytkownika hasło należy zmienić podczas pierwszego logowania, a następnie zmieniać cyklicznie po określonym czasie.	**Logiczne zarządzanie dostępem** - Klient może przez cały czas rejestrować, modyfikować, zawieszać, reaktywować i usuwać swoje profile użytkowników, a także zarządzać związanymi z nimi aspektami handlowymi (środki na koncie, progi, powiązane profile itp.). W zakresie uprawnień, każdy klient może zarządzać swoimi zasobami z administracyjnego punktu widzenia ustalając poziomy bezpieczeństwa i zarządzając przywilejami dostępu. W szczególności, w zależności od usługi, klienci mogą: • Przypisać jedną lub więcej maszyn wirtualnych do swoich użytkowników, opierając się na systemie księgowym w ramach wirtualnej maszyny. • W przypadku usług Cloud Object Storage i Cloud Backup można utworzyć unikalne poświadczenia, które zostaną przypisane do niezależnych grup zasobów. • W przypadku usługi Private Cloud możliwe jest tworzenie zestawów użytkowników technicznych posiadających różne uprawnienia w panelu sterowania technicznego. • W przypadku klientów partnerskich zawsze istnieje możliwość zdefiniowania zestawów operacji dozwolonych użytkownikom poprzez odpowiednie reguły profilowania. Uprawnienia są zorganizowane na zasadzie hierarchii: istnieją Uprawnienia „rodzica" i Uprawnienia „dziecka"; Uprawnienie „rodzica" automatycznie gwarantuje wszystkie Uprawnienia „dziecka", podczas gdy Uprawnienie „dziecka" gwarantuje tylko swoje uprawnienia i może być aktywowane nawet bez Uprawnienia „rodzica".
A.10	**Szyfrowanie**	**TLS Secure Channel** - Wszystkie przepływy danych z/do wrażliwych systemów należących do	**Kontrole szyfrowania** - Sugerujemy, aby klienci przyjęli podejście oparte na ryzyku i

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

Załącznik A - ISO 27001 Aspekty bezpieczeństwa w chmurze Grupy Aruba			
Obszar kontroli		**Nasze kontrole**	**Narzędzia i funkcje dostępne dla Klienta**
		analizowanych systemów, w szczególności serwerów eksponowanych w Internecie, są zabezpieczone przy pomocy bezpiecznego kanału TLS, poprzez odpowiednią konfigurację na serwerach, tak aby zagwarantować: • uwierzytelnienie serwera; • szyfrowanie sesji symetrycznym algorytmem szyfrującym uznanym za wystarczająco bezpieczny. Dotyczy to zarówno przepływów powstających w sposób interaktywny (przeglądanie stron internetowych), jak i generowanych automatycznie (np. zapytanie do Web Services). Dotychczas jako symetryczny algorytm szyfrujący stosowany był głównie AES. Aktywowana wersja TLS jest możliwie najwyższa, biorąc pod uwagę możliwości oprogramowania klienckiego. Certyfikaty serwera SSL instalowane na serwerach eksponowanych w Internecie są wydawane przez CA i uznawane za wiarygodne przez najpopularniejsze przeglądarki i systemy operacyjne. Szczegóły dotyczące certyfikatów używanych na panelach kontrolnych Cloud oraz protokołów używanych w sieci publicznej dostępne są w Bazie wiedzy na stronie poświęconej certyfikatom używanym na panelach kontrolnych Cloud. **Szyfrowanie Data at Rest** - Najbardziej krytyczne dla bezpieczeństwa dane pozostające „w spoczynku", takie jak hasła, pliki seed tokenów OTP i inne dane, które muszą pozostać poufne, aby zapewnić niezawodność procesów, są przechowywane przy użyciu szyfrowania symetrycznego, przy wykorzystaniu rozwiązania uważanego za wystarczająco bezpieczny algorytm. Jeśli chodzi o bardziej szczegółowe pojmowanie ochrony danych uwierzytelniających, hasła przechowuje się w ramach repozytorium w nieodwracalnym trybie „zahashowanym" (fingerprint lub digest of the data), używając algorytmu szyfrującego SHA-512.	wdrożyli dodatkowe środki kontroli szyfrowania w obszarach, za które są odpowiedzialni (patrz Matryca odpowiedzialności) w przypadku, gdy dane przetwarzane w ramach usługi świadczonej przez Grupę Aruba są szczególnie wrażliwe. **Usługa Cloud Backup – Szyfrowanie** - oferuje możliwość szyfrowania backupowanych danych zanim jeszcze zostaną przesłane za pomocą silnego hasła (standard AES-256).

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

Załącznik A - ISO 27001 Aspekty bezpieczeństwa w chmurze Grupy Aruba			
Obszar kontroli		**Nasze kontrole**	**Narzędzia i funkcje dostępne dla Klienta**
A.11	**Bezpieczeństwo fizyczne i środowiskowe**	**Centra Danych** – systemy dostarczania Usług Cloud znajdują się w Centrach Danych we Włoszech, a dokładniej w centrach danych „IT1" (Via Gobetti 96 w Arezzo), „IT2", (Via Ramelli 8 w Arezzo) oraz w centrum danych „IT3" (Via San Clemente 53 w Ponte San Pietro). Oprócz włoskich centrów danych, Grupa Aruba posiada międzynarodową sieć infrastrukturalną, zarówno własną, jak i należącą do kwalifikowanych partnerów: • Centrum danych CZ1 w Ktiš, w Republice Czeskiej, należące do międzynarodowej sieci centrów danych będących własnością Organizacji; • Centrum danych FR1, w Paryżu, we Francji, należące do sieci partnerskich centrów danych; • Centrum danych DE1, we Frankfurcie, w Niemczech, należące do sieci partnerskich centrów danych; • Centrum danych UK1, w Londynie, w Wielkiej Brytanii, należące do sieci partnerskich centrów danych; • Centrum danych PL1 w Warszawie, w Polsce, należące do sieci centrów danych partnerów. **Budynki odporne na trzęsienia ziemi** - Centra danych Grupy Aruba spełniają przepisy dotyczące odporności na trzęsienia ziemi. **Kontrola dostępu fizycznego** - Dostęp do budynków mogą mieć tylko osoby, które faktycznie go wymagają, po zarejestrowaniu się w recepcji, a dostęp do pomieszczeń technicznych jest dozwolony tylko dla upoważnionych pracowników, po identyfikacji przepustką i odpowiednim kodem PIN. System kontroli dostępu obejmuje opcję dopuszczenia i wyłączenia indywidualnych kart magnetycznych do określonych obszarów, godzin i innych kryteriów, gwarantując pełne bezpieczeństwo i łatwość dostępu. **Systemy antywłamaniowe** - W centrach danych zastosowano kraty, szyby kuloodporne, drzwi pancerne i bramy automatyczne (pasywne systemy antywłamaniowe), zainstalowano systemy telewizji przemysłowej i systemy wizyjnej detekcji ruchu (aktywne systemy antywłamaniowe). Przeciwwłamaniowy system alarmowy	

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

Załącznik A - ISO 27001 Aspekty bezpieczeństwa w chmurze Grupy Aruba			
Obszar kontroli		**Nasze kontrole**	**Narzędzia i funkcje dostępne dla Klienta**
		rozmieszczony w poszczególnych strefach działa w pełni automatycznie. Centra danych są podzielone na kilka stref, monitorowanych przez systemy antywłamaniowe. Ponadto we wszystkich obszarach centrów danych 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. **System przeciwpożarowy** - System ten został zaprojektowany dla uzyskania zgodności z przepisami oraz z odpowiednimi normami technicznymi. Czujniki wykrywające ogień są obecne na wszystkich piętrach budynków. **System przeciwpowodziowy** - Zainstalowano systemy wykrywania cieczy i przeciwpowodziowe. Budynki są również zlokalizowane na obszarach równinnych i na przemyślanej wysokości ponad poziomem gruntu. **System zasilania** - System ten jest obecny w Centrach danych i jest redundantny na wszystkich poziomach (podstacje, centra zasilania, UPS, generatory, rozdzielnice, itp.), aby zagwarantować ciągłość zasilania we wszystkich przewidywalnych warunkach. Obejmuje również środki odpowiednie dla opanowania skutków atmosferycznych wyładowań elektrycznych, skoków napięcia w sieci, itp. **Układ wentylacyjny i klimatyzacyjny (HVAC)** - Układ jest w stanie zapewnić optymalne warunki klimatyczne dla sprawnego działania serwerów hostowanych w Centrum danych. **Łączność internetowa** - W budynkach obecna jest redundantna łączność o przepustowości co najmniej dwukrotnie większej od wymaganego minimum. **Centrum Operacyjne Sieci (NOC)** - Centra danych są obsadzone przez okrągłą dobę, przez 7 dni w tygodniu, 365 dni w roku, przez wykwalifikowanych pracowników systemu, co gwarantuje stały monitoring infrastruktury i usług oraz, w razie potrzeby, szybką interwencję. **Ubezpieczenie** - Firma zawarła umowę ubezpieczeniową w celu pokrycia zagrożeń, których	

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

Załącznik A - ISO 27001 Aspekty bezpieczeństwa w chmurze Grupy Aruba			
Obszar kontroli		**Nasze kontrole**	**Narzędzia i funkcje dostępne dla Klienta**
		nie są w stanie ograniczyć inne środki bezpieczeństwa.	
A.12	**Sprzęt**	**Procedury operacyjne** - Procedury nakazujące zachowania operacyjne są udokumentowane, udostępnione i zostały przyjęte przez właściwy personel. **Server Hardening** - Serwery, na których znajdują się komponenty krytyczne dla bezpieczeństwa usług, poddawane są systemowym interwencjom mającym na celu ograniczenie obszaru ataku, takim jak: usunięcie zbędnego oprogramowania, wyłączenie niepotrzebnych usług/protokołów, zainstalowanie łatek bezpieczeństwa zalecanych przez dostawców, zastosowanie zasad dotyczących złożoności haseł, włączenie dzienników bezpieczeństwa, itp. **Ochrona przed atakiem Distributed Denial of Service (DDoS) -** Wdrożono system, który analizuje przychodzące dane, wykrywając nieprawidłowy ruch sieciowy i w miarę możliwości blokujący potencjalnie niebezpieczne pakiety. **Logi** - Logi serwerów infrastruktury dotyczące uprzywilejowanego dostępu do systemów gromadzi się i przechowuje zgodnie z wymogami prawnymi. Logi te są okresowo weryfikowane przez Zespół bezpieczeństwa w ramach wewnętrznych audytów. Logi aplikacji dotyczące operacji wykonywanych podczas korzystania z usług są udostępniane klientom. Praca Administratorów systemu podlega weryfikacji przez administratorów danych co najmniej raz w roku, w celu sprawdzenia zgodności ze środkami organizacyjnymi, technicznymi i bezpieczeństwa w zakresie przetwarzania danych osobowych, przewidzianymi na mocy obowiązujących przepisów. **Monitoring i alerty** - Krytyczne systemy Usługi są kontrolowane przez system ciągłego monitoringu. System ma możliwość generowania „alertów", w postaci wiadomości e-mail lub SMS, które umożliwiają bezzwłoczne poinformowanie odpowiedzialnych pracowników o potencjalnej awarii lub zakłóceniu, tak aby umożliwić najszybsze wprowadzenie niezbędnych działań. **Backup (w przypadkach, w których odpowiedzialność ponosi Grupa Aruba)** - W	**Backup** - Usługi w chmurze oferowane przez Grupę Aruba pozwalają klientom tworzyć i konfigurować własne zautomatyzowane kopie zapasowe przy wykorzystaniu rozwiązań Cloud Backup i Bare Metal Backup, przy wyborze własnych zasad dotyczących szyfrowania, częstotliwości, typu (pełnego lub przyrostowego) i innych specyficznych potrzeb. Opcjonalna usługa **Disaster Recovery as a Service (DRaaS)** pozwala również na testowanie procedur przejmowania funkcji bez żadnych przerw w przypadku awarii. Wszystkie procedury zarządzania usługami tworzenia kopii zapasowych i przywracania danych samodzielnie wykonują użytkownicy i opisano je w Bazie wiedzy (KB) usługi na dedykowanej stronie, gdzie opisano również metody, które można wykorzystać do tworzenia kopii zapasowych danych. Nie wykonuje się innych kopii zapasowych danych niż te niezależnie zdefiniowane przez użytkowników. **Logi** - Grupa Aruba udostępnia klientom logi aplikacji, które tworzą w ramach korzystania z usług. • Cloud PRO: użytkownik może przeglądać logi dotyczące operacji na maszynach wirtualnych, takich jak tworzenie, usuwanie, przechowywanie, przywracanie, włączanie, wyłączanie, resetowanie, zmiana haseł, zmiana funkcji, tworzenie, usuwanie i przywracanie snapshotów. • Cloud VPS (SMART): użytkownik może przeglądać logi dotyczące operacji na maszynach wirtualnych, takich jak tworzenie, usuwanie, włączanie, wyłączanie, resetowanie i uaktualnianie. • Przełączniki wirtualne: użytkownik może przeglądać logi dotyczące operacji na przełącznikach wirtualnych takich jak zakup i usunięcie oraz zmiany funkcji. • Publiczne adresy IP: użytkownik może przeglądać logi dla operacji na

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

Załącznik A - ISO 27001 Aspekty bezpieczeństwa w chmurze Grupy Aruba			
Obszar kontroli		**Nasze kontrole**	**Narzędzia i funkcje dostępne dla Klienta**
		przypadku komponentów funkcjonalnych służących do świadczenia usługi, zarządzania użytkownikami oraz innych komponentów architektury usługi stosuje się procedury tworzenia kopii zapasowych zdefiniowane na poziomie firmy, które okresowo są poddawane weryfikacji i testom. **Program antywirusowy** - Wszystkie urządzenia w sieci Grupy Aruba są kontrolowane, monitorowane i zabezpieczane przez systemy EDR. Technologia EDR (Endpoint Detection and Response) monitoruje w czasie rzeczywistym i w sposób proaktywny znane i nieznane zagrożenia we wszystkich punktach końcowych i serwerach firmowych. Dedykowana grupa dyżurująca przez całą dobę odpowiada za analizę anomalnych zdarzeń i szybką interwencję. **Proces zarządzania podatnościami** - Cały obwód Grupy Aruba jest regularnie skanowany przez zautomatyzowane narzędzia oraz przez wykwalifikowanych branżowych specjalistów w celu zidentyfikowania wszelkich prawdopodobnych lub potencjalnych podatności. Każdy zidentyfikowany krytyczny problem jest natychmiast zgłaszany do kompetentnej grupy, rozpoczynając w ten sposób cykl rozwiązywania problemów, który może doprowadzić do wydania nowej wersji lub załagodzenia (np. wirtualnym patchowaniem). Na koniec, aby zweryfikować jego skuteczność, przeprowadza się kolejne skanowanie, aby upewnić się, że system usunął podatność. **Zarządzanie pojemnością i zarządzanie zmianami** - W celu zapewnienia właściwego dostarczenia/świadczenia usługi, Grupa Aruba uważa, że niezbędne jest monitorowanie dostępnych zasobów, analizowanie pojemności i przyjęcie stosownych środków ostrożności dla ich optymalnego wykorzystania oraz zapewnienia normalnego korzystania z usług. Poziomy łączności, poziomy zajętości zasobów, przestrzeni dyskowej oraz wielkość infrastruktury są monitorowane za pomocą specjalnych narzędzi przez grupę operatorów pracujących w Centrum Operacyjnym Sieci (NOC) przez całą dobę, przez 7 dni w tygodniu, 365 dni w roku, których zadanie obejmuje również monitorowanie wszelkich anomalnych zdarzeń.	publicznych adresach IP takich jak zakup i usunięcie publicznego IP, zarządzanie i zmiana reverse DNS. • Balancery: użytkownik może przeglądać logi dla operacji na balancerach takich jak tworzenie balancera, edycja balancera, usuwanie balancera, włączanie lub wyłączanie balancera, dodawanie, edycja i usuwanie reguł. • Unified Storage: użytkownik może przeglądać logi dotyczące operacji na przełącznikach wirtualnych, takich jak zakup i usunięcie oraz zmiany funkcji. • Usługa FTP: użytkownik może przeglądać logi dla operacji na kontach FTP takich jak aktywacja i usuwanie oraz edycja przestrzeni. • Private Cloud: użytkownik może przeglądać logi dla operacji na swojej Private Cloud takich jak tworzenie, usuwanie i zmiany zasobów. • Cloud Backup: użytkownik może przeglądać logi dla operacji na swoich kontach backup związanych z tworzeniem, usuwaniem i zmianą planu, zmianą lub resetowaniem haseł. • Cloud Monitoring: użytkownik może przeglądać dzienniki operacji na swoich usługach monitorowania i powiązanych kontroli, takich jak tworzenie planu monitorowania lub dodawanie nowej kontroli, usuwanie planu monitorowania lub kontroli, zmiana planu monitorowania lub pojedynczego sprawdzenia. • Cloud Object Storage: użytkownik może przeglądać logi dla operacji na swoich kontach Object Storage związanych z tworzeniem, usuwaniem i zmianą planu, zmianą lub resetowaniem haseł. • Domain Center: użytkownik może przeglądać logi dla operacji na swoich domenach i DNS związanych z dodaniem nowej domeny, usunięciem domeny i zmianami danych domeny, utworzeniem DNS, usunięciem DNS, zmianami rekordów DNS. • Baza danych jako usługa (DBaaS): użytkownik może przeglądać logi dla operacji na swoich kontach „Database as

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

Załącznik A - ISO 27001 Aspekty bezpieczeństwa w chmurze Grupy Aruba			
Obszar kontroli		**Nasze kontrole**	**Narzędzia i funkcje dostępne dla Klienta**
		Narzędzia monitorujące umożliwiają ustalenie określonych procedur kontrolnych dla każdej usługi, wykrywanie anomalii i umożliwiają przewidywanie konieczności wprowadzenia zmian. Zmianami, które stały się konieczne w wyniku działań związanych z monitorowaniem i zarządzaniem przepustowością, zarządza się w sposób kontrolowany, aby można było zweryfikować rezultaty i śledzić przeprowadzone działania. **Uaktualnienia i łatki** - Wszystkie systemy są okresowo aktualizowane i łatane przy użyciu scentralizowanych narzędzi i zgodnie z wewnętrznymi procedurami, które wymagają ich przetestowania w pierwszej kolejności w środowiskach deweloperskich. Po zakończeniu tego etapu są one stosowane w środowisku produkcyjnym. **Synchronizacja** - Wszystkie systemy działające w chmurze wykorzystują system NTP do synchronizacji zegarów i utrzymywania spójności zdarzeń. Wiarygodnym źródłem synchronizacji zegarów jest INRiM (http://www.inrim.it). CEST to strefa czasowa stosowana we wszystkich systemach, z wyjątkiem czasu brytyjskiego, gdzie obowiązuje GMT. Wszystkie dostarczone maszyny wirtualne mają strefę czasową opartą na CEST i wykorzystują hosta, na którym są zainstalowane, jako źródło synchronizacji ich zegara. **Wieloorganizacyjność i bezpieczne usuwanie danych** - **Grupa Aruba** gwarantuje wieloorganizacyjność systemu, która umożliwia oddzielenie żądań poszczególnych klientów od siebie oraz oddzielenie żądań klientów od żądań dostawcy usług w chmurze. Grupa Aruba specjalnie opracowała panel kontrolny chmury publicznej jako rozwiązanie wykorzystujące wieloorganizacyjność zgodnie z wytycznymi dotyczącymi bezpiecznego programowania i pozwala na dostęp i kontrolę tylko własnej infrastruktury chmury klienta. Dodatkowo w przypadku usług PRO, VPS i Private Cloud oraz wszędzie, gdzie wykorzystywane jest zewnętrzne oprogramowanie, wieloorganizacyjność jest gwarantowana bezpośrednio przez stosowane systemy wirtualizacji.	a Service" związanych z tworzeniem, usuwaniem i zmianą planu, zmianą lub resetowaniem haseł, tworzeniem kopii zapasowych i przywracaniem baz danych oraz restartowaniem instancji. **Zarządzanie pojemnością** - W zakresie zarządzania pojemnością zasobów klienta, Grupa Aruba pozwala klientowi na stałe monitorowanie zużycia zasobów finansowych i technicznych, którymi dysponuje, umożliwiając również prognozowanie. Dodatkowo przy zakupie usługi podawany jest opis przypadków, w których występują ograniczenia w rozszerzalności zasobów. **Synchronizacja** - Gdy uważa się, że synchronizacja zegara może być dla klienta utrudnieniem, publiczna Baza wiedzy zawiera szczegółowe informacje (na przykład na stronie zaplanowanych operacji) lub w panelach kontrolnych. **Wieloorganizacyjność** Cloud PRO. Wieloorganizacyjność jest gwarantowana: • Przez panel sterowania chmury publicznej opracowany przez Grupę Aruba specjalnie jako rozwiązanie wspomagające wieloorganizacyjność oraz przez uwierzytelnione publiczne interfejsy API. Rozwiązania te umożliwiają wyłącznie dostęp do infrastruktury Cloud i zarządzanie nią. • Dzięki systemowi wirtualizacji Hyper-V i VMware. Klient ma dostęp tylko do swoich maszyn wirtualnych (VM), które bazowe hiperwizory utrzymują w logicznym oddzieleniu od innych. Maszyny wirtualne dostarczane klientowi są instalowane z narzędziami kontroli dostępu, których dane uwierzytelniające wybiera bezpośrednio klient podczas tworzenia. Narzędzia służące do logowania dostarczane wraz z urządzeniami to SSH dla środowisk Linux i RDP dla środowisk Windows. Sieci publiczne są przez klientów współdzielone, ale na wszystkich

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

Załącznik A - ISO 27001 Aspekty bezpieczeństwa w chmurze Grupy Aruba			
Obszar kontroli		**Nasze kontrole**	**Narzędzia i funkcje dostępne dla Klienta**
		Gdy usługa zostanie zamknięta lub gdy skończą się środki na koncie, jak określono w umowie, Grupa Aruba skasuje i trwale usunie dane z usług Cloud, jak opisano na stronie https://kb.arubacloud.pl/pl/zarzadzanie-kontem-fpl/korzystanie-ze-srodkow/co-dzieje-sie-w-przypadku-wyczerpania-srodkow.aspx. W zależności od usługi, usuwanie może odbywać się poprzez API, techniczne panele kontrolne, skrypty lub dedykowane oprogramowanie. Grupa Aruba wykorzystuje określony proces do zarządzania okresowym usuwaniem ze swoich systemów chmurowych plików tymczasowych.	udostępnionych urządzeniach znajduje się firewall do użytku klienta. Dodatkowo klient może wykupić usługę Virtual Switch, która polega na udostępnieniu dedykowanej sieci VLAN nie współdzielonej z innymi klientami, na której klient może połączyć odpowiednie urządzenia w celu maksymalnej segregacji. Cloud VPS (SMART). Wieloorganizacyjność jest gwarantowana: • Przez panel sterowania chmury publicznej opracowany przez Grupę Aruba specjalnie jako rozwiązanie wspomagające wieloorganizacyjność oraz przez uwierzytelnione publiczne interfejsy API. Rozwiązania te umożliwiają wyłącznie dostęp do infrastruktury Cloud i zarządzanie nią. • Dzięki systemowi wirtualizacji VMware. Klient ma dostęp tylko do swoich maszyn wirtualnych, które bazowe hyperwizory utrzymują w logicznej izolacji od pozostałych. Maszyny wirtualne dostarczane klientowi są instalowane z narzędziami kontroli dostępu, których dane uwierzytelniające wybiera bezpośrednio klient podczas tworzenia. Narzędzia służące do logowania dostarczane wraz z urządzeniami to SSH dla środowisk Linux i RDP dla środowisk Windows. Sieci publiczne są przez klientów współdzielone, ale na wszystkich udostępnionych urządzeniach znajduje się firewall do użytku klienta. Wirtualny Switch i Hybrid Link: są to zasoby dedykowane dla poszczególnych najemców. Wieloorganizacyjność gwarantuje panel sterowania chmury publicznej opracowany przez Grupę Aruba specjalnie jako rozwiązanie wspomagające wieloorganizacyjność oraz uwierzytelnione publiczne interfejsy API. Rozwiązania te umożliwiają jedynie dostęp do infrastruktury Cloud użytkownika i zarządzanie nią. Virtual Private Cloud. Wieloorganizacyjność jest gwarantowana:

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

Załącznik A - ISO 27001 Aspekty bezpieczeństwa w chmurze Grupy Aruba			
Obszar kontroli		**Nasze kontrole**	**Narzędzia i funkcje dostępne dla Klienta**
			• Dzięki panelowi kontrolnemu vCloud Director, specjalnie opracowanemu przez VMware do pracy w trybie wieloorganizacyjnym. Ten panel kontrolny umożliwia jedynie dostęp do infrastruktury Cloud i zarządzanie nią. • Dzięki systemowi wirtualizacji Vmware, klient ma dostęp tylko do swojego Wirtualnego centrum danych maszyny wirtualnej, które bazowe hiperwizory utrzymują w logicznej izolacji od pozostałych. Maszyny wirtualne dostarczane klientowi są instalowane z narzędziami kontroli dostępu, których dane uwierzytelniające wybiera bezpośrednio klient podczas tworzenia. Narzędzia służące do logowania dostarczane wraz z urządzeniami to SSH dla środowisk Linux i RDP dla środowisk Windows. Na każdym udostępnionym Wirtualnym centrum danych dostępna jest zapora programowa (NSX Edge), która umożliwia oddzielenie Wirtualnego centrum danych od pozostałych i pozwala klientowi skonfigurować optymalne reguły bezpieczeństwa dla poszczególnych zastosowań. Klient ma możliwość samodzielnego tworzenia dedykowanych sieci prywatnych, które nie są współdzielone z innymi klientami w celu skonfigurowania własnej architektury. W razie potrzeby sieci publiczne mogą być również zapewniane jako sieci dedykowane, nie współdzielone z innymi klientami. Bare Metal Backup. Wieloorganizacyjność jest gwarantowana: • Przez panel sterowania chmury publicznej opracowany przez Grupę Aruba specjalnie jako rozwiązanie wspomagające wieloorganizacyjność oraz przez uwierzytelnione publiczne interfejsy API. Rozwiązania te umożliwiają wyłącznie dostęp do infrastruktury Cloud i zarządzanie nią. • Przez panel kontrolny Veeam. Klienci mają dostęp tylko do własnego zbioru danych i nie mają możliwości podglądu

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

Załącznik A - ISO 27001 Aspekty bezpieczeństwa w chmurze Grupy Aruba			
Obszar kontroli		**Nasze kontrole**	**Narzędzia i funkcje dostępne dla Klienta**
			lub kontrolowania systemów backup innych klientów. Disaster Recovery. Wieloorganizacyjność jest gwarantowana: • Przez panel sterowania chmury publicznej opracowany przez Grupę Aruba specjalnie jako rozwiązanie wspomagające wieloorganizacyjność oraz przez uwierzytelnione publiczne interfejsy API. Rozwiązania te umożliwiają wyłącznie dostęp do infrastruktury Cloud i zarządzanie nią. • Przez panel kontrolny Zerto. Klienci mają dostęp tylko do własnego zbioru danych i nie mają możliwości podglądu ani kontrolowania kont Disaster Recovery (DR) innych klientów. Cloud Backup (Evault/Commvault). Wieloorganizacyjność jest gwarantowana: • Przez panel sterowania chmury publicznej opracowany przez Grupę Aruba specjalnie jako rozwiązanie wspomagające wieloorganizacyjność oraz przez uwierzytelnione publiczne interfejsy API. Rozwiązania te umożliwiają wyłącznie dostęp do infrastruktury Cloud i zarządzanie nią. • Dzięki systemowi kopii zapasowych Evault lub Commvault. Klienci mają dostęp tylko do własnego zbioru danych i nie mają możliwości podglądu lub kontrolowania systemów backup innych klientów. Cloud Monitoring: Wieloorganizacyjność gwarantuje panel sterowania chmury publicznej opracowany przez Grupę Aruba specjalnie jako rozwiązanie wspomagające wieloorganizacyjność oraz uwierzytelnione publiczne interfejsy API. Rozwiązania te umożliwiają wyłącznie dostęp do infrastruktury Cloud i zarządzanie nią. Cloud Object Storage: Wieloorganizacyjność jest gwarantowana: • Przez panel sterowania chmury publicznej opracowany przez Grupę Aruba specjalnie jako rozwiązanie

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

Załącznik A - ISO 27001 Aspekty bezpieczeństwa w chmurze Grupy Aruba			
Obszar kontroli		**Nasze kontrole**	**Narzędzia i funkcje dostępne dla Klienta**
			wspomagające wieloorganizacyjność oraz przez uwierzytelnione publiczne interfejsy API. Rozwiązania te umożliwiają wyłącznie dostęp do infrastruktury Cloud i zarządzanie nią. • Dzięki systemowi Scality Identity i Zarządzaniu dostępem. Klienci mają dostęp tylko do własnego konta pamięci masowej i nie mają możliwości podglądu ani kontrolowania kont innych klientów. Domain Center: Wieloorganizacyjność gwarantuje panel sterowania chmury publicznej opracowany przez Grupę Aruba specjalnie jako rozwiązanie wspomagające wieloorganizacyjność oraz uwierzytelnione publiczne interfejsy API. Rozwiązania te umożliwiają wyłącznie dostęp do infrastruktury Cloud i zarządzanie nią. Baza danych jako usługa (DBaaS): Wieloorganizacyjność gwarantuje panel sterowania chmury publicznej opracowany przez Grupę Aruba specjalnie jako rozwiązanie wspomagające wieloorganizacyjność oraz uwierzytelnione publiczne interfejsy API. Rozwiązania te umożliwiają wyłącznie dostęp do infrastruktury Cloud i zarządzanie nią.
A.13	**Bezpieczeństwo komunikacji**	**Firewall i IPS** - Portale internetowe udostępniane na potrzeby usług są chronione przez firewall centrum danych usług w chmurze oraz chronione przez IPS. Jeśli chodzi o usługi obliczeniowe, wszystkie maszyny wirtualne dostarczane przez Grupę Aruba są modelowane i udostępniane w postaci obrazów. Obrazy te są tworzone i testowane przez techników Grupy Aruba, a w szczególności po zainstalowaniu Systemu operacyjnego i przeprowadzeniu pierwszej konfiguracji włączany jest system zapory sieciowej, nadający możliwie najniższy poziom dostępu i otwierający tylko niezbędne protokoły. **Virtual Private Network (VPN)** - Zdalny dostęp do sieci firmowej (LAN) jest przyznawany tylko upoważnionym pracownikom, którzy potrzebują takiego dostępu; zdalny dostęp jest możliwy tylko poprzez VPN, który zapewnia: poufność komunikacji, silne uwierzytelnienie serwera i silne (dwuetapowe) uwierzytelnienie użytkownika.	**Firewall** - Klienci są administratorami własnego serwera i dlatego też mają możliwość zmiany ustawień firewalla. Przewodniki i samouczki w Bazie Wiedzy dostarczają informacji o tym, jak segregować i chronić bezpieczeństwo sieci oraz skonfigurować firewall na własnej chmurze klienta. **Wirtualny Switch -** Klienci mają możliwość wykupienia usługi Wirtualnego Switch'a, która obejmuje udostępnienie dedykowanej sieci VLAN, która nie jest współdzielona z innymi klientami, na której klienci mogą łączyć swoje maszyny dla uzyskania maksymalnej segregacji, z możliwością samodzielnego tworzenia dedykowanych sieci prywatnych, nie współdzielonych z innymi klientami, do konfiguracji własnej architektury (Private Cloud).

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

Załącznik A - ISO 27001 Aspekty bezpieczeństwa w chmurze Grupy Aruba			
Obszar kontroli		**Nasze kontrole**	**Narzędzia i funkcje dostępne dla Klienta**
			W razie potrzeby sieci publiczne mogą być również zapewniane jako sieci dedykowane, nie współdzielone z innymi klientami. **Geograficzna lokalizacja danych gwarantująca Bezpieczeństwo i zgodność** - Zamiennie, usługi dostarczane przez Grupę Aruba mogą być aktywowane na bazie centrum danych lub regionalnie (co oznacza konkretny kraj). Klienci mają możliwość określenia Centrum lub Centrów danych, w których ich usługi mają zostać aktywowane, i do których ich dane mają być przesyłane; w przypadku usług świadczonych na podstawie regionalnej, klienci mają możliwość wyboru kraju, w obrębie którego usługi mają być aktywowane. W żadnym wypadku Grupa Aruba nie przenosi systemów ani treści poza granice lokalizacji geograficznych (centrum danych lub regiony) skonfigurowanych przez swoich klientów.
A.14	**Pozyskiwanie, tworzenie i konserwacja systemów**	**Zarządzanie zmianami** - Zmiany w oprogramowaniu aplikacyjnym podlegają ocenie i zatwierdzeniu przed ich wdrożeniem; są one następnie testowane przed przejściem do produkcji, w celu sprawdzenia poprawności wdrożenia nowych funkcji i braku regresji. Ponadto, całe tworzone oprogramowanie jest zarządzane przez system wersjonowania.	**Zarządzanie zmianami** - Grupa Aruba dostarcza klientom log zmiany (jak opisano na dedykowanej stronie Bazy wiedzy), aby informować ich o wersjach, poprawkach, korektach i aktualizacjach usług.
A.15	**Relacje z dostawcami**	**Zarządzanie dostawcami** - Grupa Aruba posiada politykę korporacyjną, która reguluje relacje z dostawcami. Polityka przewiduje, że dla właściwego określenia i zarządzania relacjami z każdym nowym dostawcą należy zawsze brać pod uwagę między innymi następujące aspekty, szczególny nacisk kładąc na bezpieczeństwo informacji: • ocena ryzyka i wstępne badania, które należy przeprowadzić w celu dokonania pełnej oceny nowego dostawcy; • dobór klauzul umownych, w celu oceny, czy standardowe umowy zabezpieczają przed zidentyfikowanymi zagrożeniami, czy też może	

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

Załącznik A - ISO 27001 Aspekty bezpieczeństwa w chmurze Grupy Aruba			
Obszar kontroli		**Nasze kontrole**	**Narzędzia i funkcje dostępne dla Klienta**
		być konieczne dodanie/zmiana konkretnych klauzul; • kontrola dostępu do informacji, w celu zapewnienia dostawcy dostępu zgodnie z zasadą „Need-to-know", a więc tylko do tych danych i informacji, które są rzeczywiście wymagane i niezbędne do wykonywania odpowiednich czynności; • kontrola dostępu do systemów Grupy Aruba, jeżeli przedmiot dostawy umożliwia dostawcy dostęp do systemów, poprzez określonych użytkowników, z wykorzystaniem sieci prywatnej (VPN) i określonego systemu reagowania na wykrycie oraz wirtualnej infrastruktury desktopowej (VDI) dostarczonej przez Grupę Aruba; • monitorowanie niezgodności, w celu regularnego przeprowadzania kontroli, aby zweryfikować zgodność dostawcy z ustalonymi wymogami umownymi oraz bezpieczeństwo informacji. Dodatkowo, zewnętrzne dostawy niezbędne do rozwoju, utrzymania i świadczenia Usługi podlegają kontrolom mającym na celu ograniczenie ryzyka wystąpienia incydentów związanych z bezpieczeństwem spowodowanych przez niezgodne materiały lub niewłaściwe działania dostawców. Wszyscy dostawcy profesjonalnych usług są zobowiązani do podpisania umowy o zachowaniu poufności (NDA). Stosowane przez Grupę Aruba wzory umów dotyczących świadczenia usług przewidują możliwość korzystania przez Grupę Aruba w celu prowadzenia działalności z usług podmiotów zewnętrznych. Współpraca ta opiera się na zobowiązaniu Grupy Aruba, określonym w umowach z wszystkimi jej podwykonawcami, do weryfikacji, czy w oparciu o rodzaj świadczonej usługi są oni w stanie spełnić te same wymagania i poziomy bezpieczeństwa, do których zobowiązała się Grupa Aruba. Grupa Aruba prowadzi listę podwykonawców usług, dostępną na żądanie klientów. Podobnie, gdy zatrudniani są nowi/dodatkowi podwykonawcy, Grupa Aruba zobowiązuje się powiadomić swoich klientów z odpowiednim wyprzedzeniem, aby umożliwić tym ostatnim wniesienie zastrzeżeń lub wycofanie się.	

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

Załącznik A - ISO 27001 Aspekty bezpieczeństwa w chmurze Grupy Aruba			
Obszar kontroli		**Nasze kontrole**	**Narzędzia i funkcje dostępne dla Klienta**
A.16	**Zarządzanie zagrożeniami dla bezpieczeństwa informacji**	**Proces zarządzania incydentami związanymi z bezpieczeństwem informacji** - Grupa Aruba określiła i udokumentowała, w ramach ustalonej polityki, swoje uporządkowane i programowe podejście do zarządzania zdarzeniami i incydentami związanymi z bezpieczeństwem informacji, które mogą wystąpić w kontekście działalności spółek Grupy Aruba, stosując wytyczne normy ISO 27035 w swoich przepływach informacji z zarządzania incydentami związanymi z bezpieczeństwem informacji. Proces ten jest realizowany za pośrednictwem specjalnego planu, który określa środki operacyjne, które należy wdrożyć w przypadku Incydentów związanych z bezpieczeństwem informacji. Zdefiniowano przepływ zarządzania incydentami i określono obowiązki związane z jego stosowaniem, zarówno w zakresie zarządzania incydentami i ich rozwiązywania, jak i w zakresie wsparcia strategicznego dla terminowego podejmowania decyzji niezbędnych do rozwiązywania najistotniejszych Incydentów związanych z bezpieczeństwem (na przykład Incydentów poważnych, Incydentów nieznanych, Naruszeniami danych). Określono również harmonogramy i procedury przygotowywania i przekazywania organom, klientom i podmiotom zewnętrznym komunikatów dotyczących incydentów związanych z bezpieczeństwem informacji.	
A.17	**Aspekty bezpieczeństwa informacji związane z zarządzaniem ciągłością biznesową**	**Procedura zarządzania kryzysowego** - **Grupa Aruba** przygotowała Plan ciągłości działania oraz konkretne procedury odnoszące się do usług, które są niezbędne do funkcjonowania Centrów danych (energia elektryczna, klimatyzacja i łączność). Centra danych posiadają certyfikat ISO 27001, co oznacza, że cała infrastruktura jest chroniona za pomocą fundamentalnych środków bezpieczeństwa fizycznego i ciągłości działania. Centra danych Aruba IT1, IT3 DCA i DCB są zgodne z najwyższym poziomem (Rating 4) regulacji ANSI TIA 942-B-2017. Ocena ta wskazuje na zdolność do zapobiegania przerwom w świadczeniu usług z powodu poważnych awarii (fault-tolerance) i została osiągnięta dzięki szeregowi środków projektowych i wdrożeniowych zastosowanych we	**Disaster Recovery as a Service (DRaaS)** - **Grupa Aruba** dostarcza rozwiązanie Disaster Recovery jako usługę zaprojektowaną w celu zagwarantowania ciągłości prowadzenia działalności dla firm, umożliwiając im szybką replikację i przywrócenie dostępu i funkcjonalności ich infrastruktury IT po przerwie spowodowanej cyberatakiem, awarią lub katastrofalnym wydarzeniem. Korzystając z samoobsługowego panelu zarządzania Web z bezpiecznym połączeniem, klienci mogą tworzyć wytyczne i polityki usuwania skutków awarii, wybierając źródło (Primary Site) i miejsce docelowe (Secondary Site) z własnej infrastruktury wirtualnej VMware i centrów

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

Załącznik A - ISO 27001 Aspekty bezpieczeństwa w chmurze Grupy Aruba			
Obszar kontroli		**Nasze kontrole**	**Narzędzia i funkcje dostępne dla Klienta**
		wszystkich aspektach budowy centrum danych: wybór lokalizacji, względy architektoniczne, bezpieczeństwo fizyczne, systemy przeciwpożarowe, systemy elektryczne, sprzęt mechaniczny i sieć danych. Data center o standardzie Rating 4 (dawniej Tier 4) posiada stale aktywne nadmiarowe komponenty, a także wiele źródeł zasilania i chłodzenia sprzętu. Podsumowując, centra danych są zaprojektowane tak, aby były odporne na awarie w dowolnym obszarze obiektu, bez powodowania przestojów, są również chronione przed zagrożeniami fizycznymi, w tym klęskami żywiołowymi (np. pożary, powodzie, trzęsienia ziemi itp.). Centra danych Aruba IT3 DCA i DCB posiadają certyfikat ISO/IEC 22237, międzynarodowy standard odniesienia dla całego cyklu życia centrum danych, od koncepcji strategicznej po wdrożenie i eksploatację, zgodnie z przepisami ANSI/TIA 942 (standard amerykański) i EN 50600 (standard europejski). Środowisko Cloud obejmuje infrastrukturę wielu centrów danych, których usługi są połączone siecią o wysokiej przepustowości i ochronie IPSEC. Dzięki strukturze obejmującej wiele centrów danych, jest ona natywnie przygotowana do odzyskiwania po awarii dzięki temu, że każde centrum danych jest niezależne od pozostałych z logistycznego punktu widzenia. Zwirtualizowane serwery klienta nie podlegają geograficznemu Disaster Recovery, ponieważ klienci otrzymują wszystkie niezbędne narzędzia do tworzenia własnych, dostosowanych do indywidualnych potrzeb systemów i procedur Disaster Recovery.	danych Grupy Aruba z włączoną usługą Private Cloud.
A.18	**Zgodność**	**Ochrona danych osobowych** - Wszystkie usługi są świadczone przy zachowaniu pełnej zgodności z obowiązującymi przepisami dotyczącymi ochrony danych osobowych, zgodnie z rozporządzeniem (UE) 2016/679 ("RODO"). **Audyt** - Zdarzenia zarejestrowane za pomocą śledzenia, szczególnie te, które mogą wskazywać na zagrożenie bezpieczeństwa, są analizowane w pewnych odstępach czasowych. **Wewnętrzne inspekcje** - Kierownik ds. audytów i inspekcji upewnia się, że co najmniej raz w roku przeprowadzane są kontrole zgodności usługi w	

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

Załącznik A - ISO 27001 Aspekty bezpieczeństwa w chmurze Grupy Aruba			
Obszar kontroli		**Nasze kontrole**	**Narzędzia i funkcje dostępne dla Klienta**
		chmurze z zapisami niniejszego dokumentu i obowiązującymi przepisami.	

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** Z DNIA 14/04/2023	***CHARAKTER ZMIAN: Aktualizacja punktu A.12, A.13, A.17***
WERSJA **1.0** 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