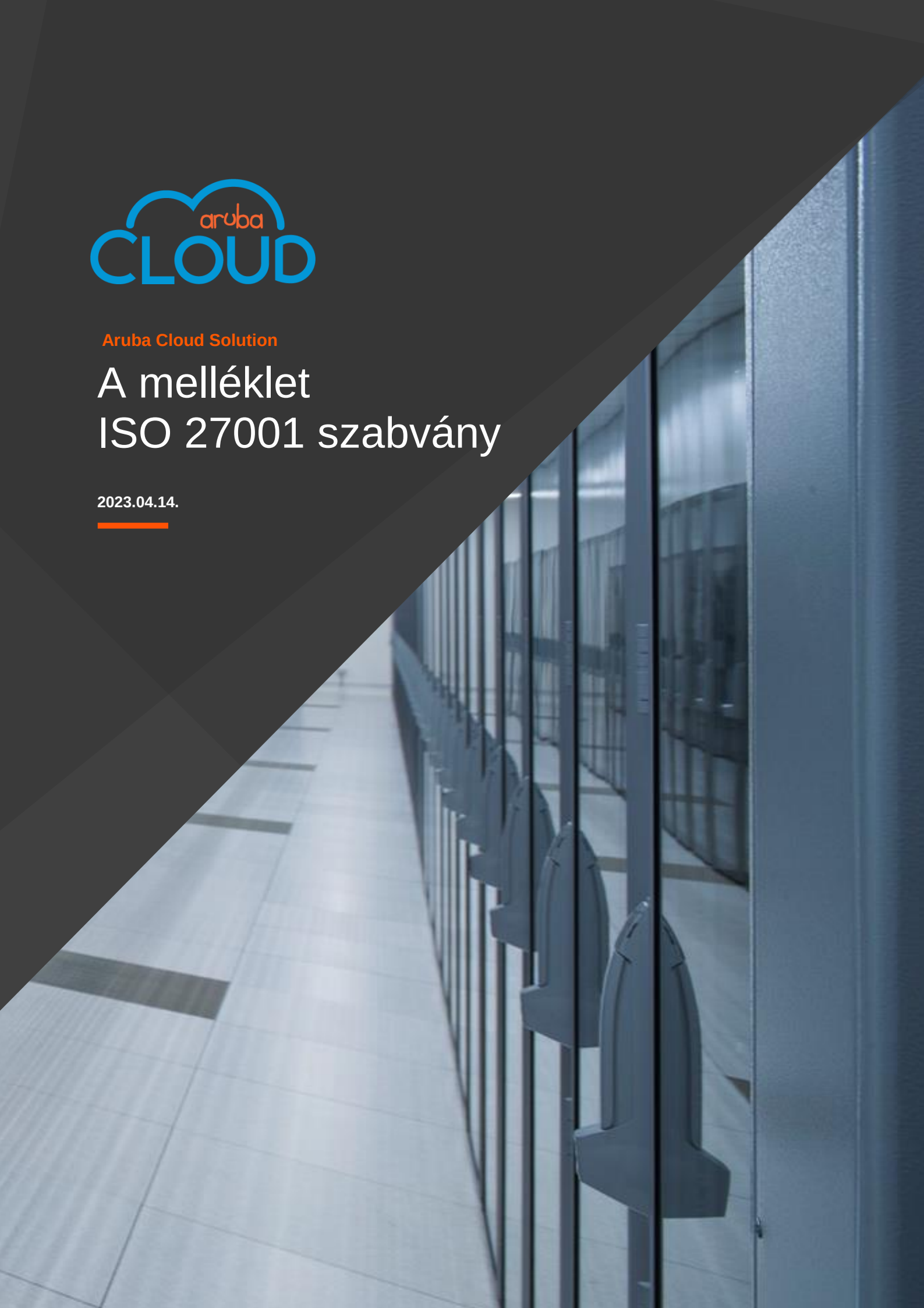
Aruba Cloud Solution

# A melléklet ISO 27001 szabvány

2023.04.14.



| A melléklet – ISO 27001 szabvány<br>Az Aruba Csoport Cloud szolgáltatásának biztonsági vonatkozásai | | | |
|---|---|---|---|
| **Ellenőrzési terület** | | **Ellenőrzési eszközeink** | **Az ügyfél számára rendelkezésre álló eszközök és funkciók** |
| **A.5** | **Adatbiztonsági szabályok** | **Az információbiztonsági irányítási rendszerre vonatkozó szabályok (**ISMS) – Az Aruba Csoport egy konkrét Vállalati Szabályzatban határozta meg a szervezet által alkalmazott megközelítést az információbiztonsági célok kezelésére. Ezt a dokumentumot jóváhagyta az Igazgatóság, és közzétette a vállalat intranet hálózatán. A fent említett Szabályzatot további szabályok és eljárások támogatják, amelyek meghatározzák az Aruba Csoport adatbiztonsági irányítási rendszerét. | |
| **A.6** | **Az adatbiztonság felépülése** | **Feladatok és felelősségvállalás** – Felhőszolgáltatóként a közös felelősségi modellnek szentelt oldalon meghatározott felelősségi körén belül az Aruba Csoport meghatározta az adott folyamatokat ellátó személyzetet, szerepeket, készségeket és felelősségi köröket, a feladatok elkülönítésének, a legkisebb jogosultságnak és a kettős ellenőrzésnek az elveivel összhangban.<br><br>**A feladatok elkülönítése (SoD)** – A Szolgáltatások működési folyamatainak keretein belül különböző személyek különböző eljárásokat hajtanak végre, így a teljes folyamatot nem irányíthatja egyetlen személy.<br><br>**A legkisebb jogosultság** – A helyiségekhez, berendezésekhez, adatokhoz, funkciókhoz stb. való hozzáférés a szolgáltatásokra kijelölt személyzet számára a „legkisebb jogosultság” elvének megfelelően engedélyezett, azaz csak és kizárólag olyan mértékben, amely szükséges a rájuk bízott feladatok elvégzéséhez.<br><br>**Kettős ellenőrzés** – A biztonsági szempontból legkritikusabb eljárásokat legalább két személy végzi. | **Feladatok és felelősségvállalás** – A szolgáltatás általános leírása megtalálható a Tudásbázisban (KB), a szolgáltatás általános leírásának szentelt oldalon, a szolgáltatás teljesítési helyének táblázatával és az Aruba Csoport, mint Felhőszolgáltató és ügyfelei között megosztott felelősségi modellt bemutató táblázattal együtt. |
| **A.7** | **HR-biztonság** | **Az alkalmazottak képzése** –A szolgáltatást nyújtó személyzet megfelelő készségekkel és tapasztalattal rendelkezik, és minden fontos rendszerfrissítéshez speciális képzést kap.<br><br>**Tudatosság** – Az alkalmazottak rendszeres időközönként tájékoztatásban részesülnek a biztonsági kérdésekről, a számítástechnikai bűnözésről általában és a végrehajtandó bevált gyakorlatokról, speciális képzések keretében. | **Képzés és tudatosság** – Az Aruba Csoport biztosít egy, a felhőszolgáltatásokkal kapcsolatos információkat tartalmazó Tudásbázist, amely információkat tartalmaz a szolgáltatásokról, útmutatókról, oktatóanyagokról, az Alkalmazásprogramozási interfészekről (API) szóló dokumentációról, a szószedetről és a szolgáltatások Changelog naplójáról. |



**BlazeArts Kft.**
1096 Budapest, Thaly Kálmán utca 39. cégjegyzékszám: 01-09-389087
adószám: 12539833-2-43 közösségi adószám: HU12539833
www.arubacloud.hu

| A melléklet – ISO 27001 szabvány<br>Az Aruba Csoport Cloud szolgáltatásának biztonsági vonatkozásai | | | |
|---|---|---|---|
| **Ellenőrzési terület** | | **Ellenőrzési eszközeink** | **Az ügyfél számára rendelkezésre álló eszközök és funkciók** |
| | | **Titoktartási szerződés (NDA)** – Az újonnan felvett alkalmazottaknak titoktartási szerződést kell aláírnia a vállalat know-how-jának és egyéb bizalmas információinak védelme érdekében. | |
| **A.8** | **Eszközkezelés** | **Eszközleltár** – Az eszközökről naprakész leltár készül, amely tartalmazza a szolgáltatásokat nyújtó virtuális és fizikai berendezések nyilvántartását, valamint fizikai elhelyezkedésüket az Aruba Csoport infrastruktúráján belül.<br><br>Az eszközök leltára az infrastruktúra minden egyes új berendezésének telepítése után frissítésre kerül. Ezenfelül az eltérések ellenőrzése érdekében a hálózatok automatikus szkennelése naponta történik az új eszközök észlelése érdekében.<br><br>A leltár tartalmazza azoknak az eszközöknek a leírását, amelyekben a releváns jellemzők szerepelnek: például a berendezés típusa (virtuális vagy fizikai), az infrastruktúra, amelyhez tartozik, a belső tulajdonos, stb.<br><br>**Eszközök kezelése** – Olyan belső eljárásokkal is rendelkezünk, amelyek meghatározzák és formalizálják az új berendezések előkészítésével és kezelésével kapcsolatos tevékenységeket (pl., hogy hogyan kell változást végrehajtani, hogyan kell frissíteni a rendszereket, stb.).<br><br>**Konfigurációkezelés** – A rendszerösszetevők felsorolása úgy került meghatározásra, hogy lehetővé tegye az egyes hardver- és szoftverösszetevők, illetve azok modelljének vagy verziójának azonosítását.<br><br>**Karbantartás és támogatás** – A Szolgáltatás folyamatossága szempontjából a legfontosabb hardver (HW) komponensekre karbantartási szerződések vonatkoznak, amelyek garantálják a szállító általi javítást vagy cserét kellően rövid időn belül, vagy az azonos tárolt komponensek rendelkezésre állását, amelyek szükség esetén telepíthetők. Ami a kereskedelmi szoftvereket (SW) illeti, léteznek megfelelő támogatási szerződések, amelyek meghibásodás esetén garantálják a szállító műszaki támogatását.<br><br>**Ártalmatlanítás** – Az Aruba Csoport garantálja, hogy speciális eljárásokat alkalmaz a már nem használt hardverösszetevők megsemmisítésére mind a külföldi adatközpontokban, mind a saját | **Tulajdonjog** – A közös felelősség elvével összhangban az Aruba Csoport minden egyes szolgáltatás esetében azonosította a tulajdonviszonyokat az infrastruktúra, a licencek, az IP-címek, az Aruba Csoport által biztosított szoftverek, az ügyfél által bevitt szoftverek, adatok és tartalom tekintetében.<br><br>A szolgáltatások eszközeinek tulajdonjogára vonatkozó információk az ügyfelek számára a nyilvános tudásbázison belül az annak szentelt oldalon érhetők el.<br><br>**Adatok törlése** – A felhőkörnyezetben, a VPS (Smart), PRO és Virtual Private Cloud szolgáltatások esetében a lemeztörlési technika használatával az ügyfélnek lehetősége van arra, hogy véglegesen törölje a berendezésén tárolt adatokat, és lehetetlenné tegye azok helyreállítását. A tudásbázis ennek szentelt oldala ismerteti a műveleti lépéseket.<br><br>**Címkézés** – Az Aruba Csoport szolgáltatásai lehetővé teszik az ügyfelek számára, hogy az általuk ellenőrzött eszközöket megnevezzék és osztályozzák. A Tudásbázisban közzétett útmutatók pontos utasításokat adnak a műveletek végrehajtásáról és a korlátozásokról. |



**BlazeArts Kft.**
1096 Budapest, Thaly Kálmán utca 39. cégjegyzékszám: 01-09-389087
adószám: 12539833-2-43 közösségi adószám: HU12539833
www.arubacloud.hu

| A melléklet – ISO 27001 szabvány<br>Az Aruba Csoport Cloud szolgáltatásának biztonsági vonatkozásai | | | |
|---|---|---|---|
| **Ellenőrzési terület** | | **Ellenőrzési eszközeink** | **Az ügyfél számára rendelkezésre álló eszközök és funkciók** |
| | | tulajdonú adatközpontokban annak biztosítása érdekében, hogy minden olyan tárolóösszetevő esetében, amely elérte az élettartama végét, és amelyet ki kell cserélni és meg kell semmisíteni, az abban foglalt összes adat teljes mértékben és véglegesen törlésre kerüljön. | |
| **A.9** | **A hozzáférés ellenőrzése** | **A hozzáférés logikai kezelése** – A belső rendszerekhez való hozzáférés előtt a felhatalmazott személyzetnek azonosítania és hitelesítenie kell magát (felhasználónévvel, jelszóval és/vagy okoskártyával). A hitelesítést követően az Aruba Csoport személyzete csak azokhoz az erőforrásokhoz (pl. rendszerekhez, adatokhoz) férhet hozzá, amelyekre kifejezetten felhatalmazták, a beosztásuk tényleges igényeinek megfelelően. A felhasználók kezelése az Active Directory (AD) tartományvezérlőkön keresztül történik. A „feladatelkülönítés" elvének biztosítása érdekében a termelési környezethez való logikai hozzáférés kezelése AD-n keresztül történik egy dedikált tartományban, amelyen belül a felhasználók különböző jogosultságokkal és engedélyekkel rendelkeznek az adott személy munkaköri szerepével összhangban, a legkisebb jogosultság elvének megfelelően. Minden felhasználó egy egyénnek felel meg, így nincsenek csoport- és/vagy megosztott felhasználók, és a Biztonsági Osztály rendszeresen független ellenőrzésnek veti őket alá.<br><br>**A jelszóhasználat szabálya** – A csoport biztonsági irányelveivel és az adatvédelmi jogszabályokkal („minimumintézkedések", az adatvédelmi hatóság rendelkezései) összhangban biztonságos jelszókezelési politikát alkalmazunk.<br>A felhasználó létrehozását követően a jelszót az első bejelentkezéskor, majd egy meghatározott idő elteltével rendszeresen meg kell változtatni. | **A hozzáférések logikai kezelése** – Az ügyfél bármikor regisztrálhatja, módosíthatja, felfüggesztheti, újraaktiválhatja és törölheti felhasználói profilját, valamint kezelheti a kapcsolódó kereskedelmi tényezőket (kreditek, küszöbértékek, kapcsolódó profilok, stb.). Az engedélyek tekintetében minden ügyfél kezelheti eszközeit adminisztrációs szempontból a biztonsági szintek beállításával és a hozzáférési jogosultságok kezelésével. A szolgáltatástól függően az ügyfelek számára lehetséges:<br>• egy vagy több virtuális gép hozzárendelése a felhasználókhoz, a virtuális gépen belüli számviteli rendszer támogatásával;<br>• a Cloud Object Storage és Cloud Backup szolgáltatások esetében lehetőség van egyedi hitelesítő adatok létrehozására, amelyek független erőforráscsoportokhoz rendelhetők hozzá;<br>• a Virtual Private Cloud szolgáltatáshoz különböző jogosultságokkal rendelkező technikai felhasználók csoportjai hozhatók létre a műszaki vezérlőpulton;<br>• a partner ügyfelek számára mindig lehetséges a felhasználók számára engedélyezett műveletek meghatározása a megfelelő profilalkotási szabályok révén.<br><br>Az engedélyek hierarchikusan vannak elrendezve. |
| **A.10** | **Titkosítás** | **TLS Biztonságos csatorna** – A felügyeleti rendszerekből származó/rendszerekbe irányuló valamennyi adatáramlást TLS biztonságos csatorna védi, a szerverek megfelelő konfigurációja révén, a következők biztosítása érdekében:<br>• a szerver hitelesítése; | **A titkosítás ellenőrzése** – Javasoljuk, hogy az ügyfelek kockázatalapú megközelítést alkalmazzanak, és további titkosítási ellenőrzéseket hajtsanak végre azokon a területeken, amelyekért felelősek (lásd a Felelősségi mátrixot) abban az esetben, ha az Aruba Csoport szolgáltatásán belül feldolgozott adatok különösen érzékenyek. |



**BlazeArts Kft.**
1096 Budapest, Thaly Kálmán utca 39. cégjegyzékszám: 01-09-389087
adószám: 12539833-2-43 közösségi adószám: HU12539833
www.arubacloud.hu

| A melléklet – ISO 27001 szabvány<br>Az Aruba Csoport Cloud szolgáltatásának biztonsági vonatkozásai | | | |
|---|---|---|---|
| **Ellenőrzési terület** | | **Ellenőrzési eszközeink** | **Az ügyfél számára rendelkezésre álló eszközök és funkciók** |
| | | • munkamenet-titkosítás kellően biztonságosnak tartott szimmetrikus titkosítási algoritmussal.<br><br>Ez vonatkozik mind az interaktívan (webböngészés), mind az automatikusan keletkező (pl. webszolgáltatások lekérdezése) folyamatokra.<br><br>Mostanáig az AES elsősorban szimmetrikus titkosítási algoritmusként szolgált.<br><br>A TLS engedélyezett verziója a lehető legmagasabb, figyelembe véve a ügyfelek szoftverjeinek képességeit.<br><br>Az interneten elérhető szerverekre telepített SSL szervertanúsítványokat a fő böngészők és operációs rendszerek által megbízhatónak elismert hitelesítésszolgáltató adja ki.<br><br>A felhőalapú vezérlőpultokon használt tanúsítványok részletei és a nyilvános hálózaton használt protokollok a tudásbázisban érhetők el a felhőalapú vezérlőpultokon használt tanúsítványoknak szentelt oldalon.<br><br>**Passzív adatok titkosítása** – A biztonság szempontjából legkritikusabb "passzív" adatokat, mint például a jelszavakat, az OTP token seedeket és más olyan adatokat, amelyeknek bizalmasnak kell maradniuk a folyamatok megbízhatóságának biztosítása érdekében, szimmetrikus titkosítással tárolják, egy biztonságosnak ítélt algoritmus segítségével.<br><br>Ami a hitelesítő adatok védelmét illeti, a jelszavakat az adattárban nem visszafejthető „hash” módban (ujjlenyomat vagy az adatok kivonata) tárolják az SHA 512 hash algoritmus segítségével. | **Cloud Backup – titkosítás** – A Cloud Backup szolgáltatás lehetővé teszi, hogy a biztonsági mentés alatt álló adatokat még átvitel előtt összetett jelszóval titkosítsa (AES 256 szabvány). |
| **A.11** | **Fizikai és környezeti biztonság** | **Adatközpontok** – A felhőszolgáltatást biztosító rendszerek az IT1 és az IT2 adatközpontokban találhatók Arezzoban, a Via Gobetti 96-ban és a Via Ramelli 8-ban, valamint az IT3 DCA és DCB adatközpontjaiban Ponte San Pietroban (BG), a Via San Clemente 53-ban. Az olaszországi adatközpontok mellett az Aruba Csoport nemzetközi infrastruktúra hálózattal is rendelkezik, amely saját tulajdonú és minősített partnerekhez tartozik:<br><br>• CZ1 adatközpont Ktišban, Csehországban, amely a Csoport tulajdonában lévő adatközpontok nemzetközi hálózatához tartozik; | |

| A melléklet – ISO 27001 szabvány<br>Az Aruba Csoport Cloud szolgáltatásának biztonsági vonatkozásai | | | |
|---|---|---|---|
| **Ellenőrzési terület** | | **Ellenőrzési eszközeink** | **Az ügyfél számára rendelkezésre álló eszközök és funkciók** |
| | | • FR1 adatközpont Párizsban, Franciaországban, amely a partner adatközpontok hálózatához tartozik;<br>• DE1 adatközpont Frankfurtban, Németországban, amely a partner adatközpontok hálózatához tartozik;<br>• UK1 adatközpont Londonban, az Egyesült Királyságban, amely a partner adatközpontok hálózatához tartozik;<br>• PL1 adatközpont Varsóban, Lengyelországban, amely a partner adatközpontok hálózatához tartozik.<br>**Földrengésálló épületek** – Az Aruba Csoport adatközpontjai megfelelnek az antiszeizmikus előírásoknak.<br>**A fizikai hozzáférés ellenőrzése** – Az épületekbe csak azok léphetnek be, akiknek ténylegesen szükségük van rá, a recepción történő bejelentkezéssel, a technikai helyiségekbe való belépés pedig csak az arra jogosult személyek számára engedélyezett, a belépőkártyával és a megfelelő PIN-KÓDDAL történő azonosítást követően. A beléptető rendszer lehetővé teszi az egyedi húzókártyák engedélyezését és letiltását bizonyos területeken, időpontokban és egyéb kritériumoknak megfelelően, garantálva a teljes biztonságot és a könnyű hozzáférést.<br>**Behatolásgátló rendszerek** – Az összes adatközpontban és irodában rácsok, golyóálló üveg, páncélozott ajtók és motoros kapuk (passzív behatolásgátló rendszerek) vannak telepítve, valamint CCTV és VMD rendszereket (aktív behatolásgátló rendszerek) alkalmazunk. A különböző zónákban a behatolásgátló riasztórendszer teljesen automatikus.<br>Az adatközpontok több zónára oszlanak, amelyeket behatolásgátló rendszerek felügyelnek. Emellett mozgásérzékelőket telepítettünk minden területre, amelyek képesek érzékelni az emberek jelenlétét; az érzékeny területeken (adatszobák, áramellátó központok, raktárak) is vannak olyan érzékelők, amelyek érzékelik az ajtók nyitását.<br>**Tűzoltó rendszer** – Ezt a rendszert úgy tervezték, hogy megfeleljen a törvénynek és a vonatkozó | |



**BlazeArts Kft.**
1096 Budapest, Thaly Kálmán utca 39. cégjegyzékszám: 01-09-389087
adószám: 12539833-2-43 közösségi adószám: HU12539833
www.arubacloud.hu

| A melléklet – ISO 27001 szabvány<br>Az Aruba Csoport Cloud szolgáltatásának biztonsági vonatkozásai | | | |
|---|---|---|---|
| **Ellenőrzési terület** | | **Ellenőrzési eszközeink** | **Az ügyfél számára rendelkezésre álló eszközök és funkciók** |
| | | műszaki szabványoknak. A tűzérzékelők az épületek minden emeletén jelen vannak.<br><br>**Árvízvédelmi rendszer** – Folyadékérzékelő és árvízvédelmi rendszerek vannak telepítve. Az épületek sík területeken és a környezethez képest megemelt helyen helyezkednek el.<br><br>**Tápellátó rendszer** – Ez a rendszer jelen van az adatközpontokban, és minden szinten (alállomások, áramellátó központok, szünetmentes tápegységek, generátorok, kapcsolótáblák, stb.) redundáns, hogy minden előre látható körülmény között garantálja az áramellátás folyamatosságát. Megfelelő intézkedéseket is tartalmaz a légköri elektromos kisülések, hálózati tüskék, stb. hatásának megfékezésére.<br><br>**Szellőztető és légkondicionáló rendszer (HVAC)** – A rendszer képes optimális hőmérsékleti feltételeket biztosítani az adatközpontokban tárolt szerverek zökkenőmentes működéséhez.<br><br>**Internetcsatlakozás** – Redundáns összeköttetés van jelen az épületekben, a minimálisan szükséges kapacitás legalább kétszeresével.<br><br>**Hálózati Operációs Központ (NOC)** – Az adatközpontokat a nap 24 órájában, az év 365 napján szakképzett rendszerszemélyzet felügyeli, amely biztosítja az infrastruktúra és a szolgáltatások folyamatos ellenőrzését, valamint szükség esetén az időben történő beavatkozást.<br><br>**Biztosítás** – Az Aruba Csoport biztosítási szerződést kötött azon kockázatok fedezésére, amelyeket más biztonsági intézkedések nem enyhítenek. | |
| **A.12** | **A berendezés** | **Működési szabályzat** – A működési viselkedést előíró eljárások dokumentáltak, elérhetőek és az érintett személyzet által ismertek.<br><br>**Szervervédelem** – A szolgáltatások biztonsága szempontjából kritikus komponenseket kiszolgáló szerverek rendszerszintű beavatkozásokon mennek keresztül, amelyek célja a támadási felület csökkentése, például: szükségtelen szoftverek eltávolítása, szükségtelen szolgáltatások/protokollok letiltása, a vendor-ok által ajánlott biztonsági javítások telepítése, a jelszavak bonyolultságára vonatkozó irányelvek alkalmazása, biztonsági naplók engedélyezése, stb. | **Biztonsági mentés** – Az Aruba Csoport által kínált felhőszolgáltatások lehetővé teszik az ügyfelek számára, hogy saját automatizált biztonsági mentéseket készítsenek és hozzanak létre a Cloud Backup és a Bare Metal Backup megoldásokon keresztül, kiválasztva saját szabályaikat a titkosítás, a gyakoriság, a típus (teljes vagy inkrementális) és más speciális igények tekintetében.<br><br>A **Disaster Recovery as a Service** kiegészítő szolgáltatás **(DRaaS)** lehetővé teszi a feladatátvételi eljárások megszakítás nélküli tesztelését is.<br><br>A biztonsági mentési és visszaállítási szolgáltatások kezelésének minden eljárását a felhasználók önállóan |

| A melléklet – ISO 27001 szabvány<br>Az Aruba Csoport Cloud szolgáltatásának biztonsági vonatkozásai | | | |
|---|---|---|---|
| **Ellenőrzési terület** | | **Ellenőrzési eszközeink** | **Az ügyfél számára rendelkezésre álló eszközök és funkciók** |
| | | **Elosztott szolgáltatásmegtagadással járó támadások (DDoS) elleni védelem –** Egy rendszer, amely elemzi a beérkező adatokat, észleli a rendellenes forgalmat, és ahol lehetséges, blokkolja a potenciálisan veszélyes csomagokat.<br><br>**Naplózás** – Az infrastrukturális szervernaplók összegyűjtése és tárolása a rendszerekhez való privilegizált hozzáférés érdekében a törvényi előírásoknak megfelelően történik. Ezeket a naplókat a biztonsági csapat rendszeres időközönként belső ellenőrzéseknek veti alá. A szolgáltatások igénybevétele során végzett műveletek alkalmazásnaplóit az ügyfelek rendelkezésére bocsátjuk.<br><br>Hasonlóképpen, a Rendszergazdák munkáját az adatkezelők évente legalább egyszer ellenőrzik annak érdekében, hogy felülvizsgálják a személyes adatok feldolgozására vonatkozó szervezeti, technikai és biztonsági intézkedések betartását, amelyeket a hatályos rendeletek előírnak.<br><br>**Felügyelet és riasztások** – A Szolgáltatás kritikus rendszereit folyamatos felügyeleti rendszer vezérli. A rendszer képes „riasztásokat" generálni e-mail vagy SMS formájában, amelyek lehetővé teszik, hogy azonnal tájékoztassa a potenciális balesetért vagy zavarért felelős személyzetet, hogy a szükséges intézkedéseket a lehető leghamarabb végre lehessen hajtani.<br><br>**Biztonsági mentés (amikor az Aruba Csoport a felelős)** – A szolgáltatás nyújtásához szükséges funkcionális komponensek, a felhasználókezelés és a szolgáltatás egyéb architekturális komponensei a vállalati szinten meghatározott biztonsági mentési eljárásokat követik, amelyeket rendszeresen ellenőrzünk és tesztelünk.<br><br>**Antivírus** – Az Aruba Csoport hálózatának minden eszközét EDR rendszerek vezérlik, felügyelik és védik. Az EDR (Endpoint Detection and Response, végpont-felismerés és válasz) technológia valós időben és proaktívan figyeli az ismert és ismeretlen fenyegetéseket az összes végponton és vállalati szerveren. A 24 órás lefedettséggel rendelkező dedikált csoport felelős a rendellenes események elemzéséért és az azonnali beavatkozásért.<br><br>**A sebezhetőség kezelésének folyamata** – Az Aruba Csoport teljes területe rendszeres átvizsgáláson | végzik, és a szolgáltatás Tudásbázisában (KB) ismertetik az annak szentelt oldalon, ahol az adatok biztonsági mentéséhez használható különböző módszereket is leírják.<br><br>Az adatokról semmilyen más biztonsági másolat nem készül, kivéve azokat, amelyeket a felhasználók önállóan határoznak meg.<br><br>**Naplózás** – Az Aruba Csoport biztosítja az ügyfeleknek a szolgáltatások igénybevétele során általuk készített alkalmazásnaplókat.<br><br>• Cloud PRO: a felhasználó megtekintheti a virtuális gépeken végzett műveletek naplóit, például létrehozásokról, törlésekről, tárolásokról, visszaállításokról, bekapcsolásokról, kikapcsolásokról, jelszómódosításokról, megváltozott funkciókról, valamint pillanatfelvételek létrehozásáról, törléséről és visszaállításáról.<br>• Cloud VPS (SMART): a felhasználó megtekintheti a virtuális gépeken végzett műveletek naplóit, például a létrehozásokról, törlésekről, bekapcsolásokról, kikapcsolásokról, visszaállításokról és frissítésekről.<br>• Virtuális Switch-ek: a felhasználó megtekintheti a virtuális kapcsolókon végzett műveletek naplóit, például az aktiválásokat és az eltávolításokat, valamint a változásokat.<br>• Nyilvános IP-k: a felhasználó megtekintheti a nyilvános IP-címeken végzett műveletek naplóit, például a nyilvános IP-címek megvásárlását és eltávolítását, a reverse DNS kezelését és megváltoztatását.<br>• Terheléselosztók: a felhasználó megtekintheti a kiegyensúlyozó műveletek naplóit, például a kiegyensúlyozó létrehozását, a kiegyensúlyozó szerkesztését, a kiegyensúlyozó törlését, a kiegyensúlyozó engedélyezését vagy letiltását, a szabályok hozzáadását, szerkesztését és eltávolítását.<br>• Unified Storage: a felhasználó megtekintheti a virtuális switch műveleteinek naplóit, például a aktiválást és az eltávolítást, valamint a változást.<br>• FTP szolgáltatás: a felhasználó megtekintheti az FTP fiókon végzett műveletek naplóit, például aktiválásokról, eltávolításokról és szerkesztésekről.<br>• Virtual Private Cloud: a felhasználó megtekintheti a Virtual Private Cloud szolgáltatásban végzett |



**BlazeArts Kft.**
1096 Budapest, Thaly Kálmán utca 39. cégjegyzékszám: 01-09-389087
adószám: 12539833-2-43 közösségi adószám: HU12539833
www.arubacloud.hu

| A melléklet – ISO 27001 szabvány<br>Az Aruba Csoport Cloud szolgáltatásának biztonsági vonatkozásai | | | |
|---|---|---|---|
| **Ellenőrzési terület** | | **Ellenőrzési eszközeink** | **Az ügyfél számára rendelkezésre álló eszközök és funkciók** |
| | | esik át automatizált eszközökkel és szakirányú képzettséggel rendelkező szakemberekkel a lehetséges vagy potenciális sebezhetőségek azonosítása érdekében. Minden azonosított kritikus problémát azonnal jelentenek az illetékes csoportnak, ezzel elindítva egy problémamegoldó ciklust, amely új szoftver kiadás vagy más biztonsági mechanizmus alkalmazásával zárul (pl. virtual patching). Végül, a hatékonyság ellenőrzése végett egy másik vizsgálat történik, hogy megbizonyosodjunk a rendszer helyreállásáról.<br><br>**A kapacitás és a változások kezelése** – A szolgáltatás megfelelő nyújtásának biztosítása érdekében az Aruba Csoport úgy véli, hogy alapvető fontosságú a rendelkezésre álló erőforrások figyelemmel kísérése, a kapacitások elemzése és a megfelelő óvintézkedések elfogadása azok optimális kihasználása és a szolgáltatások rendes használatának biztosítása érdekében.<br><br>A kapcsolódási szinteket, az erőforrás-elfoglaltság szintjét, a lemezterületet és az infrastruktúra méretezését speciális eszközökkel figyeli a Hálózati Operációs Központhoz (NOC) tartozó üzemeltetők csoportja az év minden napján és a nap minden órájában, amelynek feladata kiterjed a rendellenes események megfigyelésére is.<br><br>A felügyeleti eszközök lehetővé teszik az egyes szolgálatokra vonatkozó egyedi ellenőrzések meghatározását, a rendellenességek észlelését és a változás szükségességének előrejelzését.<br><br>A felügyeleti és kapacitáskezelési tevékenységek által szükségessé tett változtatásokat ellenőrzött módon kezelik, hogy az eredmények ellenőrizhetők legyenek, és hogy nyomon lehessen követni az elvégzett tevékenységeket.<br><br>**Frissítések és javítások** – Minden rendszer rendszeres frissítésen és javításon megy keresztül központosított eszközökkel és belső eljárásokat követve, amelyek először tesztelést igényelnek a fejlesztési környezetben. Miután ez a lépés befejeződött, a termelési környezetben kerülnek alkalmazásra.<br><br>**Szinkronizálás** – Minden felhőalapú rendszer az NTP rendszert használja az órák szinkronizálására és az eseménykonzisztencia fenntartására. Az óraszinkronizálás hiteles forrása az INRiM | műveletek naplóit, például az erőforrások létrehozásáról, törléséről és módosításairól.<br>• Cloud Backup: a felhasználó megtekintheti a biztonsági mentéshez használt fiókon végzett folyamatok naplóit, például a díjcsomag aktiválásával, törlésével és módosításával, illetve a jelszó megváltoztatásával és visszaállításával kapcsolatban.<br>• Cloud Monitoring: a felhasználó megtekintheti a monitoring szolgáltatásain végzett műveletek és a kapcsolódó ellenőrzések naplóit, mint például egy monitoring díjcsomag létrehozásáról vagy új ellenőrzés hozzáadásáról, egy monitoring díjcsomag vagy ellenőrzés törléséről, a monitoring díjcsomag vagy egy ellenőrzés módosításáról.<br>• Cloud Object Storage: a felhasználó megtekintheti az Object Storage fiókjában a díjcsomag létrehozásával, törlésével és módosításával, jelszavak módosításával vagy visszaállításával kapcsolatos műveletek naplóit.<br>• Domain Center: megtekintheti a domain nevein és a DNS-én végzett műveletek naplóit az új domain hozzáadásával, a domain törlésével és a domain adatok módosításával, a DNS létrehozásával, a DNS törlésével, valamint a DNS rekordok változásaival kapcsolatban.<br>• Jelastic Cloud: a felhasználó megtekintheti a Jelastic Cloud fiókjában a díjcsomag létrehozásával, törlésével és módosításával, jelszavak módosításával vagy visszaállításával kapcsolatos műveletek naplóit.<br>• Database as a Service (DBaaS): a felhasználó megtekintheti az "DBaaS" fiókjaik műveleteinek naplóit, amelyek a díjcsomag létrehozásával, törlésével és módosításával, a jelszavak megváltoztatásával vagy visszaállításával, az adatbázisok biztonsági mentésével és visszaállításával, valamint a szolgáltatások újraindításával kapcsolatosak.<br><br>**Kapacitáskezelés** – Az Aruba Csoport az ügyfélkapacitás-kezelést illetően lehetővé teszi, hogy az ügyfél folyamatosan nyomon kövesse a rendelkezésére álló pénzügyi és technikai erőforrások felhasználását, lehetővé téve az előrejelzést is.<br><br>Emellett a szolgáltatás megvásárlásakor leírást adunk azokról az esetekről, amikor az erőforrások bővíthetősége korlátozott. |



**BlazeArts Kft.**
1096 Budapest, Thaly Kálmán utca 39. cégjegyzékszám: 01-09-389087
adószám: 12539833-2-43 közösségi adószám: HU12539833
www.arubacloud.hu

| A melléklet – ISO 27001 szabvány<br>Az Aruba Csoport Cloud szolgáltatásának biztonsági vonatkozásai | | | |
|---|---|---|---|
| **Ellenőrzési terület** | | **Ellenőrzési eszközeink** | **Az ügyfél számára rendelkezésre álló eszközök és funkciók** |
| | | (www.inrim.it). Az összes használt rendszer időzónája a CEST, kivéve az Egyesült Királyságban, ahol a GMT-t használják. Minden rendelkezésre bocsátott VMS rendelkezik CEST alapú időzónával, és azt a gazdaállomást használja az óra szinkronizálásának forrásaként, amelyre telepítették őket.<br><br>**Multitenant architektúra és biztonságos adattörlés – Az Aruba Csoport** olyan többfelhasználós rendszert garantál, amely lehetővé teszi az egyes ügyfelek kéréseinek egymástól való elkülönítését, valamint az ügyfelek kéréseinek a Felhőszolgáltató kéréseitől való elkülönítését.<br><br>Az Aruba Csoport a nyilvános cloud control panelt kifejezetten a biztonságos programozásra vonatkozó irányelvekkel összhangban fejlesztette ki, és csak az ügyfél saját felhőinfrastruktúrájának elérését és vezérlését teszi lehetővé. Ezenkívül a PRO, VPS és Virtual Private Cloud szolgáltatások esetében, valamint külső szoftverek használata esetén a többszintű használatot közvetlenül a használt virtualizációs rendszerek garantálják.<br><br>Amikor a szolgáltatás megszűnik, vagy amikor a kreditegyenleg kimerül a szerződésben meghatározottak szerint, az Aruba Csoport törli és véglegesen eltávolítja az adatokat a Cloud szolgáltatásokból a kb.arubacloud.hu/hu/fhu-fiok-kezelese/kredit-hasznalat/mi-tortenik-ha-a-kredit-elfogy.aspx oldalon leírtak szerint. A szolgáltatástól függően a törlés API-k, control panelek, szkriptek vagy speciális szoftverek segítségével történhet.<br><br>Az Aruba Csoport meghatározott folyamatot alkalmaz az ideiglenes fájlok cloud rendszereiből történő időszakos törlésének kezelésére. | **Szinkronizálás** – Ha úgy gondoljuk, hogy az óra szinkronizálása nehézségekbe ütközhet az ügyfél számára, a nyilvános Tudásbázisban (például az ütemezett műveletek oldalán) vagy a vezérlőpaneleken részletes információk találhatók.<br><br>**Multitenant architektúra**<br><br>Cloud PRO<br>Garantáljuk a multitenant architektúrát:<br><br>• A pubblikus control panel segítségével, amely exkluzív az Aruba Csoport számára került kifejlesztésre a multitenant architektura és a hitelesitett nyilvános API-k által. Ezek a megoldások csak a cloud alapú infrastruktúra elérését és irányítását teszik lehetővé.<br>• A Hyper-V és VMware virtualizációs rendszer által. Az ügyfél csak a virtuális gépeihez (VM-ekhez) fér hozzá, amelyeket az alapul szolgáló hipervizorok logikailag elszigetelnek a többiektől. Az ügyfélnek biztosított virtuális gépek olyan hitelesítő eszközökkel vannak telepítve, amelyek hitelesítési adatait az ügyfél közvetlenül választja ki a létrehozás során. A gépekhez biztosított bejelentkezési lehetőség a linux környezet esetében az SSH, a windows környezet esetében az RDP. A nyilvános hálózatokat megosztják az ügyfelek, azonban az összes rendelkezésre álló berendezést külső tűzfal védi az ügyfelek számára. Ezenfelül az ügyfélnek lehetősége van megvásárolni a Virtual Switch szolgáltatást, amely egy dedikált, más ügyfelekkel nem megosztott VLAN szolgáltatásból áll, amelyen az ügyfél összekapcsolhatja a megfelelő berendezéseket a maximális elkülönítés érdekében.<br><br>Cloud VPS (SMART)<br>Garantáljuk a multitenant architektúrát:<br><br>• A pubblikus control panel segítségével, amely exkluzív az Aruba Csoport számára került kifejlesztésre a multitenant architektura és a hitelesitett nyilvános API-k által. Ezek a megoldások csak a cloud alapú infrastruktúra elérését és irányítását teszik lehetővé.<br>• A VMware virtualizációs rendszer által. Az ügyfél csak a virtuális gépeihez (VM-ekhez) fér hozzá, amelyeket az alapul szolgáló hipervizorok logikailag elszigetelnek a többiektől. Az ügyfélnek biztosított virtuális gépek olyan hitelesítő eszközökkel vannak telepítve, amelyek hitelesítési |

| A melléklet – ISO 27001 szabvány<br>Az Aruba Csoport Cloud szolgáltatásának biztonsági vonatkozásai | | | |
|---|---|---|---|
| **Ellenőrzési terület** | | **Ellenőrzési eszközeink** | **Az ügyfél számára rendelkezésre álló eszközök és funkciók** |
| | | | adatait az ügyfél közvetlenül választja ki a létrehozás során. A gépekhez biztosított bejelentkezési lehetőség a linux környezet esetében az SSH, a windows környezet esetében az RDP. A nyilvános hálózatokat megosztják az ügyfelek, azonban az összes rendelkezésre álló berendezést külső tűzfal védi az ügyfelek számára.<br><br>Virtual Switch and Hybrid Link: ezek az egyes felhasználóknak szánt erőforrások. A pubblikus control panel segítségével, amely exkluzív az Aruba Csoport számára került kifejlesztésre a multitenant architektura és a hitelesitett nyilvános API-k által. Ezek a megoldások csak a cloud infrastruktúra elérését és irányítását teszik lehetővé.<br><br>Virtual Private Cloud<br>Garantáljuk a multitenant architektúrát:<br>• A vCloud Director control panellel, amelyet kifejezetten a VMware fejlesztett ki multitenant módban. Ez a control panel csak a cloud infrastruktúra elérését és irányítását teszi lehetővé.<br>• A VMware virtualizációs rendszer által. Az ügyfél csak a virtuális gépeihez fér hozzá a saját Virtuális Adatközpontján belül, amelyeket az alapul szolgáló hipervizorok logikailag elszigetelnek a többiektől. Az ügyfélnek biztosított virtuális gépek olyan hitelesítő eszközökkel vannak telepítve, amelyek hitelesítési adatait az ügyfél közvetlenül választja ki a létrehozás során. A gépekhez biztosított bejelentkezési lehetőség a linux környezet esetében az SSH, a windows környezet esetében az RDP. Minden biztosított virtuális adatközpontban elérhető egy külső tűzfal (NSX Edge), amely lehetővé teszi a virtuális adatközpont elszigetelését a többitől, és lehetővé teszi az ügyfél számára, hogy az adott célokhoz optimális biztonsági szabályokat állítson be. Az ügyfélnek lehetősége van önállóan dedikált magánhálózatokat létrehozni, amelyeket más ügyfelekkel nem oszt meg azok saját architektúrájának konfigurálásához. Szükség esetén a nyilvános hálózatok dedikált hálózatokként is biztosíthatók, amelyek nem kerülnek megosztásra más ügyfelekkel.<br><br>Bare Metal Backup<br>Garantáljuk a multitenant architektúrát: |



**BlazeArts Kft.**
1096 Budapest, Thaly Kálmán utca 39. cégjegyzékszám: 01-09-389087
adószám: 12539833-2-43 közösségi adószám: HU12539833
www.arubacloud.hu

| A melléklet – ISO 27001 szabvány<br>Az Aruba Csoport Cloud szolgáltatásának biztonsági vonatkozásai | | | |
|---|---|---|---|
| **Ellenőrzési terület** | | **Ellenőrzési eszközeink** | **Az ügyfél számára rendelkezésre álló eszközök és funkciók** |
| | | | • A pubblikus control panel segítségével, amely exkluzív az Aruba Csoport számára került kifejlesztésre a multitenant architektura és a hitelesitett nyilvános API-k által. Ezek a megoldások csak a cloud alapú infrastruktúra elérését és irányítását teszik lehetővé.<br>• A Veeam vezérlőpult által. Az ügyfelek csak a saját biztonsági mentési adatkészletükhöz férhetnek hozzá, és nem férhetnek hozzá vagy ellenőrizhetik más ügyfelek biztonsági mentési rendszereit.<br><br><u>Disaster Recovery</u><br>Garantáljuk a multitenant architektúrát:<br><br>• A pubblikus control panel segítségével, amely exkluzív az Aruba Csoport számára került kifejlesztésre a multitenant architektura és a hitelesitett nyilvános API-k által. Ezek a megoldások csak a cloud alapú infrastruktúra elérését és irányítását teszik lehetővé.<br>• A Zero vezérlőpult által. Az ügyfelek csak a saját adatkészletükhöz férhetnek hozzá, és nem férhetnek hozzá vagy ellenőrizhetik más ügyfelek katasztrófa utáni helyreállítási (DR) rendszereit.<br><br><u>Cloud Backup (Evault/Commvault)</u><br>Garantáljuk a multitenant architektúrát:<br><br>• A pubblikus control panel segítségével, amely exkluzív az Aruba Csoport számára került kifejlesztésre a multitenant architektura és a hitelesitett nyilvános API-k által. Ezek a megoldások csak a cloud alapú infrastruktúra elérését és irányítását teszik lehetővé.<br>• Az Evault vagy Commvault biztonsági mentési rendszer által. Az ügyfelek csak a saját biztonsági mentési adatkészletükhöz férhetnek hozzá, és nem férhetnek hozzá vagy ellenőrizhetik más ügyfelek biztonsági mentési rendszereit.<br><br><u>Cloud Monitoring:</u> A pubblikus control panel segítségével, amely exkluzív az Aruba Csoport számára került kifejlesztésre a multitenant architektura és a hitelesitett nyilvános API-k által. Ezek a megoldások csak a cloud alapú infrastruktúra elérését és irányítását teszik lehetővé.<br><br><u>Cloud Object Storage</u><br>Garantáljuk a multitenant architektúrát:<br><br>• A pubblikus control panel segítségével, amely exkluzív az Aruba Csoport számára került kifejlesztésre a multitenant architektura és a |

| A melléklet – ISO 27001 szabvány<br>Az Aruba Csoport Cloud szolgáltatásának biztonsági vonatkozásai | | | |
|---|---|---|---|
| **Ellenőrzési terület** | | **Ellenőrzési eszközeink** | **Az ügyfél számára rendelkezésre álló eszközök és funkciók** |
| | | | hitelesitett nyilvános API-k által. Ezek a megoldások csak a cloud alapú infrastruktúra elérését és irányítását teszik lehetővé.<br>• A Scality Identity és az Access Management rendszer által. Az ügyfelek csak a saját tároló fiókjukhoz férhetnek hozzá, és nem férhetnek hozzá vagy ellenőrizhetik más ügyfelek fiókjait.<br><br>Domain Center: Több módszerrel garantáljuk a multitenant architektúrát: A pubblikus control panel segítségével, amely exkluzív az Aruba Csoport számára került kifejlesztésre a multitenant architektura és a hitelesitett nyilvános API-k által. Ezek a megoldások csak a cloud alapú infrastruktúra elérését és irányítását teszik lehetővé.<br><br>Jelastic Cloud. A multitenant architektúra kétféle módon biztosított:<br><br>• A pubblikus control panel segítségével, amely exkluzív az Aruba Csoport számára került kifejlesztésre a multitenant architektura és a hitelesitett nyilvános API-k által. Ezek a megoldások csak a cloud alapú infrastruktúra elérését és irányítását teszik lehetővé.<br>• A Jelastic rendszerből az ügyfelek csak a saját Jelastic fiókjukhoz férhetnek hozzá, és nem férhetnek hozzá vagy ellenőrizhetik más ügyfelek fiókjait.<br><br>Database as a Service (DBaaS): Több módszerrel garantáljuk a multitenant architektúrát: A pubblikus control panel segítségével, amely exkluzív az Aruba Csoport számára került kifejlesztésre a multitenant architektura és a hitelesitett nyilvános API-k által. Ezek a megoldások csak a cloud alapú infrastruktúra elérését és irányítását teszik lehetővé. |
| **A.13** | **Kommunikációbiztonság** | **Tűzfal és IPS** – A szolgáltatásokhoz biztosított webportálokat a felhőszolgáltatás adatközponti tűzfala és IPS védi.<br><br>Ami a cloud computing szolgáltatásokat illeti, az Aruba Csoport által biztosított összes virtuális gép sablonját lemezkép formájában teszik elérhetővé. Ezeket a lemezképeket az Aruba Csoport technikusai készítik és tesztelik, az operációs rendszer telepítése és az első konfiguráció elvégzése után engedélyezik a tűzfalrendszert, a | **Tűzfal** – Az ügyfelek a saját szerverük adminisztrátorai, ezért módosíthatják a tűzfal beállításait. A tudásbázisban található útmutatók és oktatóanyagok tájékoztatást nyújtanak a hálózati biztonság elkülönítéséről és védelméről, valamint tűzfal beállításáról az ügyfél saját felhőjében.<br><br>**Virtuális Switch** Az ügyfeleknek lehetőségük van megvásárolni a Virtuális Switch szolgáltatást, amely magában foglalja egy dedikált VLAN biztosítását, amelyet nem osztanak meg más ügyfelekkel, és amelyen az ügyfelek összekapcsolhatják gépeiket a |



**BlazeArts Kft.**
1096 Budapest, Thaly Kálmán utca 39. cégjegyzékszám: 01-09-389087
adószám: 12539833-2-43 közösségi adószám: HU12539833
www.arubacloud.hu

| A melléklet – ISO 27001 szabvány<br>Az Aruba Csoport Cloud szolgáltatásának biztonsági vonatkozásai | | | |
|---|---|---|---|
| **Ellenőrzési terület** | | **Ellenőrzési eszközeink** | **Az ügyfél számára rendelkezésre álló eszközök és funkciók** |
| | | lehető legkevesebb jogosultság biztosításával, és csak a szükséges portok megnyitásával.<br><br>**Virtual Private Network (VPN)** – A vállalati hálózathoz (LAN) csak az erre feljogosított személyzet férhet hozzá; távoli hozzáférés csak olyan VPN-en keresztül lehetséges, amely biztosítja a kommunikáció bizalmasságát, az erős szerverhitelesítést és az erős (kétfaktoros) felhasználói hitelesítést. | maximális elkülönítés érdekében, és önállóan hozhatnak létre dedikált magánhálózatokat, amelyeket más ügyfelekkel nem oszt meg azok saját architektúrájának konfigurálásához (Private Cloud).<br><br>Szükség esetén a nyilvános hálózatok dedikált hálózatokként is biztosíthatók, amelyek nem kerülnek megosztásra más ügyfelekkel.<br><br>**Az adatok földrajzi elhelyezkedése a biztonság és a megfelelőség biztosítása érdekében** – Alternatív megoldásként az Aruba Csoport által nyújtott szolgáltatások adatközpont alapján vagy regionálisan (ország alapján) is aktiválhatók.<br><br>Az ügyfeleknek lehetőségük van megadni azt az Adatközpontot vagy azokat az Adatközpontokat, amelyekben szolgáltatásaikat aktiválni és adataikat továbbítani kívánják; a regionális alapon nyújtott szolgáltatások esetében az ügyfeleknek lehetőségük van kiválasztani, hogy melyik országon belül aktiválják a szolgáltatást.<br><br>Az Aruba Csoport semmilyen körülmények között nem helyezi át rendszereit vagy tartalmait az ügyfelei által konfigurált földrajzi helyeken (adatközpontokon vagy régiókon) kívülre. |
| **A.14** | **Rendszerbeszerzés, -fejlesztés és -karbantartás** | **A változások kezelése** – Az alkalmazásszoftver változásait végrehajtásuk előtt ki kell értékelni és jóvá kell hagyni; tesztelik őket a használat megkezdése előtt, hogy ellenőrizzék az új funkciók helyes megvalósítását. Ezenfelül az összes kifejlesztett szoftvert egy verziókezelő rendszer kezeli. | **A változások kezelése** – Az Aruba Csoport (a dedikált tudásbázis oldalon leírtak szerint) változásnaplót biztosít ügyfeleinek, hogy tájékoztassa őket a szolgáltatások kiadásairól, javításairól és frissítéseiről. |
| **A.15** | **A beszállítókkal való kapcsolat** | **A beszállítók kezelése** – Az Aruba Csoport vállalati szabályzattal rendelkezik, amely meghatározza a beszállítókkal fenntartott kapcsolatokat. A szabályzat előírja, hogy az egyes új beszállítókkal való kapcsolatok megfelelő meghatározásához és kezeléséhez többek között a következő szempontokat kell figyelembe venni, különös tekintettel az adatbiztonságra:<br><br>• kockázatértékelés és előzetes vizsgálatok elvégzése az új beszállító teljeskörű értékeléséhez;<br><br>• a szerződési záradékok kiválasztása, annak értékelése érdekében, hogy a szabványszerződések fedezik-e az azonosított | |

| A melléklet – ISO 27001 szabvány<br>Az Aruba Csoport Cloud szolgáltatásának biztonsági vonatkozásai | | | |
|---|---|---|---|
| **Ellenőrzési terület** | | **Ellenőrzési eszközeink** | **Az ügyfél számára rendelkezésre álló eszközök és funkciók** |
| | | kockázatokat, vagy szükség lehet-e konkrét záradékok hozzáadására/módosítására;<br>• az információkhoz való hozzáférés ellenőrzése, hogy a „Need-to-know" elvnek megfelelően biztosítsunk hozzáférést a beszállítónak, tehát csak azokhoz az adatokhoz és információkhoz, amelyek az adott tevékenység elvégzéséhez ténylegesen szükségesek;<br>• az Aruba Csoport rendszereihez való hozzáférés ellenőrzése, ha a beszerzés megköveteli a szállítótól, hogy meghatározott felhasználókon keresztül hozzáférjen a rendszerekhez az Aruba Csoport által biztosított magánhálózaton (VPN) és a virtuális asztali infrastruktúrán (VDI) található detection response system rendszer használatával;<br>• a nem megfelelőségek nyomon követése, az ellenőrzések rendszeres elvégzése annak igazolása érdekében, hogy a beszállító megfelel-e az elfogadott szerződéses követelményeknek, valamint az adatbiztonságnak.<br><br>Ezenfelül, a Szolgáltatás fejlesztéséhez, karbantartásához és nyújtásához szükséges külső kellékeket olyan ellenőrzéseknek vetjük alá, amelyek célja a nem megfelelő anyagok vagy a beszállítók nem megfelelő intézkedései által okozott biztonsági incidensek kockázatának csökkentése. Minden beszállítónak titoktartási megállapodást (NDA) kell aláírnia.<br><br>Az Aruba Csoport által a szolgáltatásnyújtás során alkalmazott szerződéses modellek lehetőséget adnak arra, hogy az Aruba Csoport harmadik feleket is igénybe vegyen tevékenysége ellátásához. Ez az együttműködés az Aruba Csoportnak az alvállalkozókkal kötött szerződésekben rögzített kötelezettségvállalásán alapul, hogy igazolják, hogy a nyújtott szolgáltatás típusától függően képesek megfelelni ugyanazoknak a követelményeknek és biztonsági szinteknek, amelyek mellett az Aruba Csoport elkötelezte magát. Az Aruba Csoport listát vezet a szolgáltató alvállalkozóiról, amely az ügyfelek kérésére rendelkezésre bocsátható. Hasonlóképpen, új/további alvállalkozók felvételekor az Aruba Csoport vállalja, hogy jó előre értesíti ügyfeleit annak érdekében, hogy ez | |

| A melléklet – ISO 27001 szabvány<br>Az Aruba Csoport Cloud szolgáltatásának biztonsági vonatkozásai | | | |
|---|---|---|---|
| **Ellenőrzési terület** | | **Ellenőrzési eszközeink** | **Az ügyfél számára rendelkezésre álló eszközök és funkciók** |
| | | utóbbiak kifogást emelhessenek vagy visszaléphessenek. | |
| **A.16** | **Az adatbiztonsági incidensek kezelése** | **Az adatbiztonsági incidensek kezelésének folyamata** – Az Aruba Csoport azonosította és egy meghatározott politikán belül dokumentálta strukturált és programozott megközelítését az Aruba Csoport vállalatainak működésével összefüggésben előforduló információbiztonsági események és incidensek kezelésére, az ISO 27035 szabványt alkalmazva adatbiztonsági incidenskezelési folyamatában.<br><br>Ez a folyamat egy konkrét terv alapján kerül végrehajtásra, amely meghatározza az adatbiztonsági incidensek esetén végrehajtandó operatív intézkedéseket.<br><br>Meghatároztuk az incidenskezelési folyamatot és az alkalmazásához kapcsolódó felelősségeket, mind az incidenskezelés és -megoldás, mind pedig a legfontosabb biztonsági incidensek (pl. jelentősebb incidensek, ismeretlen események, adatszivárgások) kezeléséhez szükséges döntések időben történő meghozatalához szükséges stratégiai támogatás tekintetében.<br><br>Az adatbiztonsági incidensekkel kapcsolatos kommunikáció előkészítésére és eljuttatására a hatóságoknak, ügyfeleknek és harmadik feleknek határidőket és eljárásokat is meghatároztunk. | |
| **A.17** | **Az üzletmenet-folytonosság kezelésének adatbiztonsági szempontjai** | **Katasztrófakezelési eljárás** – Az Aruba Csoport üzletmenet-folytonossági tervet és konkrét eljárásokat dolgozott ki az adatközpontok működéséhez nélkülözhetetlen szolgáltatásokkal (áram, légkondicionálás és hálózati kapcsolat) kapcsolatban.<br><br>Az adatközpontok ISO 27001 tanúsítvánnyal rendelkeznek, ami azt jelenti, hogy minden infrastruktúrát az elsődleges fizikai biztonsági és üzletmenet-folytonossági intézkedések védenek.<br><br>Pontosabban, az Aruba IT1, IT3 DCA és DCB adatközpontjai mind megfelelnek az ANSI TIA 942-B-2017 szabályozás legmagasabb (Rating 4) szintjének. Ez a minősítés a súlyos hibák miatti szolgáltatáskimaradások megelőzésére való képességet jelzi (hibatűrés), és ezt olyan az adatközpont építésének minden aspektusára alkalmazott tervezési és megvalósítási | **Disaster Recovery as a Service (DRaaS) –** Az Aruba Csoport a Disaster Recovery as a Service szolgáltatást kínálja, amely az üzletmenet-folytonosságát hivatott garantálni a vállalatoknak, lehetővé téve számukra, hogy az informatikai infrastruktúra gyors replikálását és az elérhetőség és a funkcionalitás visszaállítását IT-támadás, hiba vagy katasztrofális esemény miatti megszakadást követően.<br><br>Egy biztonságos kapcsolatolattal rendelkező önállóan használható webpanelen keresztül, az ügyfél saját magának hozhat létre katasztrófa-helyreállítási irányelveket és szabályzatokat, kiválasztva a forrást (elsődleges helyszín) és a célhelyet (másodlagos helyszín), hogy válasszon saját helyszíni VMware virtuális infrastruktúrái és/ vagy az Aruba Csoport adatközpontjai közül, amelyek engedélyezve vannak a Virtual Private Cloud szolgáltatáshoz. |

| A melléklet – ISO 27001 szabvány<br>Az Aruba Csoport Cloud szolgáltatásának biztonsági vonatkozásai | | | |
|---|---|---|---|
| **Ellenőrzési terület** | | **Ellenőrzési eszközeink** | **Az ügyfél számára rendelkezésre álló eszközök és funkciók** |
| | | intézkedések sorozatával érték el mint, helyszínválasztás, építészeti szempontok, fizikai biztonság, tűzmegelőző rendszerek, elektromos rendszerek, gépészeti berendezések és adathálózat.<br><br>A Rating 4 (korábban Tier 4) szabályozásnak megfelelő adatközpontok a hardverek többszörös energiaellátása és tartalék hűtőegységei mellett folyamatosan aktív redundáns összetevőket tartalmaznak.<br><br>Összefoglalva, az adatközpontokat úgy tervezték, hogy ellenálljanak a létesítmény bármely területén fellépő hibáknak anélkül, hogy leállást okoznának, és védettek legyenek a fizikai kockázatokkal szemben, beleértve a természeti katasztrófákat (pl. tüzek, áradások, földrengések stb.). Az Aruba Csoport IT3 DCA és DCB adatközpontjai ISO/IEC 22237 tanúsítvánnyal rendelkeznek és teljes életciklusuk során megfelelnek az adatközpontokra vonatkozó nemzetközi standardnak, a stratégiai koncepciótól a felépítésig és üzemeltetésig, összhangban az ANSI/TIA 942 (amerikai) és EN 50600 (európai) szabványokkal.<br><br>A felhő környezet egy több adatközpontból álló infrastruktúra, amelynek szolgáltatásait nagy sávszélességű és biztonságos IPSEC hálózat köti össze.<br><br>Több adatközpontból álló szerkezeti kialakításának köszönhetően natívan fel van készítve a Disaster Recovery-re azáltal, hogy logisztikai szempontból minden adatközpont független a többitől.<br><br>Az ügyfél virtualizált szerverei nem tartoznak a földrajzi alapú katasztrófa utáni helyreállítás hatálya alá, mivel maguk az ügyfelek rendelkeznek minden szükséges eszközzel a saját testre szabott Disaster Recovery rendszerük és eljárásaik létrehozásához. | |
| **A.18** | **Megfelelőség** | **A személyes adatok védelme** – Valamennyi szolgáltatás teljes mértékben megfelel a személyes adatok védelmére vonatkozó hatályos előírásoknak, az Európai Unió 679/2016 rendelet („GDPR") és az Adatvédelmi Hatóság rendelkezéseivel összhangban. | |

| A melléklet – ISO 27001 szabvány<br>Az Aruba Csoport Cloud szolgáltatásának biztonsági vonatkozásai | | | |
|---|---|---|---|
| **Ellenőrzési terület** | | **Ellenőrzési eszközeink** | **Az ügyfél számára rendelkezésre álló eszközök és funkciók** |
| | | **Ellenőrzés** – A nyomon követéssel rögzített eseményeket, különösen azokat, amelyek biztonsági fenyegetést jelezhetnek, rendszeres időközönként elemezzük.<br><br>**Belső átvilágítások** – A ellenőrzési és vizsgálati vezető gondoskodik arról, hogy a felhőszolgáltatás jelen dokumentumban foglaltaknak és a hatályos előírásoknak való megfelelését legalább évente egyszer ellenőrizzék. | |



**BlazeArts Kft.**
1096 Budapest, Thaly Kálmán utca 39. cégjegyzékszám: 01-09-389087
adószám: 12539833-2-43 közösségi adószám: HU12539833
www.arubacloud.hu

# VERZIÓTÖRTÉNET

| | |
|---|---|
| **VERZIÓ**<br>**1.1**<br>14/04/2023 | ***VÁLTOZÁS JELLEGE: A.12, A.17 szekciók frissítve*** |
| **VERZIÓ**<br>**1.0**<br>01/01/2022 | ***VÁLTOZÁS JELLEGE: Első kiadás*** |



**BlazeArts Kft.**
1096 Budapest, Thaly Kálmán utca 39. cégjegyzékszám: 01-09-389087
adószám: 12539833-2-43 közösségi adószám: HU12539833
www.arubacloud.hu