Cloud forpsi
INTERNET CZ, a.s.

Cloud Security

Príloha A
ISO 27001:2017

14/04/2023

Príloha A – ISO 27001:2017 Bezpečnostné aspekty cloudu Aruba Group			
Kontrolovaná oblasť		**Naše kontroly**	**Nástroje a funkcie dostupné pre zákazníkov**
A.5	**Pravidlá zabezpečenia informácií**	**Pravidlá systému riadenia zabezpečenia informácií (**ISMS) – Skupina Aruba Group definovala prístup, ktorý organizácia prijala na riadenie svojich cieľov ohľadom informačnej bezpečnosti v špecifickej firemnej politike. Tento dokument bol schválený manažmentom a zverejnený na intranete spoločnosti. Na podporu vyššie uvedených pravidiel existujú ďalšie pravidlá a postupy týkajúce sa konkrétnych problémov, ktoré definujú systém riadenia informačnej bezpečnosti skupiny Aruba Group.	
A.6	**Organizácia informačnej bezpečnosti**	**Úlohy a povinnosti** – V rámci svojich povinností ako poskytovateľ cloudových služieb, ako je definované na stránke venovanej modelu spoluzodpovednosti, Aruba Group definovala personál, úlohy, schopnosti a povinnosti spojené s procesmi v súlade s princípom rozdeľovania úloh, základného práva a dvojnásobnej kontroly. **Prerozdeľovanie úloh (SoD)** – V rámci prevádzkových procesov služieb, rôzne osoby vykonávajú rôzne úkony, takže žiadna osoba nemá kontrolu nad celým procesom. **Základné právo** – Povolenie na prístup do priestorov, ku zariadeniam, údajom, funkciám atď. sa udeľuje personálu, ktorému je pridelený úkon v súlade s princípom „základného práva“, t. j. v rozsahu potrebnom na to, aby tieto osoby mohli vykonávať úlohy, ktoré im boli pridelené, ale nič viac. **Dvojnásobná kontrola** – Na najkritickejšie postupy z hľadiska bezpečnosti treba súčinnosť aspoň dvoch osôb.	**Úlohy a povinnosti** – Všeobecný popis služieb možno nájsť vo vedomostnej databáze (KB) , na stránke venovanej všeobecnému popisu služieb spolu so súpisom miesta doručenia služby a súpisom zobrazujúcim model spoločnej zodpovednosti medzi Aruba Group ako poskytovateľom cloudových služieb a jej zákazníkmi.
A.7	**Bezpečnosť osôb**	**Školenie personálu** – Servisný personál má primerané zručnosti a skúsenosti, a pri každej dôležitej aktualizácii systému sa mu poskytuje špecifické školenie. **Prehľad**– Zamestnanci sú prostredníctvom špecifických školení pravidelne informovaní o bezpečnostných otázkach, počítačovej kriminalite vo všeobecnosti a o osvedčených postupoch, ktoré je potrebné prijať. **Dohoda o mlčanlivosti (NDA)** – Novoprijatí zamestnanci sú povinní podpísať dohodu o	**Školenia a prehľad** – Aruba Group poskytuje vedomostnú databázu obsahujúcu informácie o cloudových službách. Obsahuje informácie o službách, príručky, návody, dokumentáciu k aplikačným programovým rozhraniam (API), glosár a denník vykonaných zmien.

INTERNET CZ, a. s.
Ktiš 2, 384 03 Ktiš IČO: 26043319 DIČ: CZ26043319
https://www.forpsicloud.cz - https://www.forpsicloud.sk

Príloha A – ISO 27001:2017 Bezpečnostné aspekty cloudu Aruba Group			
Kontrolovaná oblasť		**Naše kontroly**	**Nástroje a funkcie dostupné pre zákazníkov**
		mlčanlivosti, aby sa ochránilo know-how spoločnosti a ďalšie dôverné informácie.	
A.8	**Správa aktív**	**Inventarizácia majetku** – Existuje aktualizovaný súpis aktív, čo zahŕňa záznam o virtuálnom a fyzickom zariadení poskytujúcom služby a ich fyzické umiestnenie v rámci infraštruktúry skupiny Aruba Group. Súpis majetku sa aktualizuje po každej inštalácii nového zariadenia v infraštruktúre. Okrem toho sa na kontrolu akýchkoľvek odchýlok vykonáva každodenné automatické skenovanie sietí, aby sa odhalili akékoľvek nové aktíva. Súpis obsahuje popis majetku, v ktorom sú popísané zodpovedajúce charakteristiky: napríklad typ zariadenia (virtuálne alebo fyzické), infraštruktúra do ktorej patrí, interné vlastníctvo atď. **Nakladanie s majetkom** – Takisto existujú interné postupy, ktoré definujú a utvárajú činnosti súvisiace s prípravou nového vybavenia a jeho spravovania (napr. ako zmeniť alebo aktualizovať systémy atď.). **Spravovanie konfigurácie** – Zoznam komponentov systému je definovaný tak, aby umožňoval identifikáciu jednotlivých hardvérových a softvérových komponentov a ich modelu alebo verzie. **Údržba a podpora**– Najdôležitejšie hardvérové (HW) komponenty poskytujúce nepretržitosť služby sú pokryté zmluvami o údržbe, ktoré zaručujú opravu alebo výmenu v dostatočne rýchlom časovom rámci dodávateľom, alebo dostupnosť identických uložených komponentov, ktoré je možné v prípade potreby nasadiť. Pokiaľ ide o komerčný softvér (SW), existujú príslušné zmluvy o podpore, ktoré zaručujú technickú podporu dodávateľa v prípade poruchy. **Vyradenie** - Spoločnosť Aruba Group garantuje, že sú prijaté postupy na vyradenie a likvidáciu hardvérových komponentov, ktoré sa už nepoužívajú pre zahraničné hosťovacie datacentrá, ako aj pre vlastnícke datacentrá, aby sa zabezpečilo, že pre každý úložný komponent, ktorý dosiahol koniec svojej životnosti a je potrebné ho	**Vlastníctvo aktív** - V súlade s princípom spoluzodpovednosti, pre každú službu Aruba Group identifikovala príslušné prisúdenia vlastníctva, pokiaľ ide o infraštruktúru, licencie, IP adresy, softvér poskytovaný skupinou Aruba, softvér, údaje a obsah zadaný zákazníkom. Informácie o vlastníctve aktív pre služby sú dostupné zákazníkom v rámci verejnej KB na vyhradenej stránke. **Vymazanie údajov** – Pomocou techniky vymazania disku v cloudovom prostredí má zákazník pri službách VPS (Smart), PRO a Private Cloud možnosť natrvalo vymazať údaje obsiahnuté vo svojom zariadení a znemožniť aby sa obnovili. Na stránke venovanej kB sú uvedené prevádzkové kroky. **Označovanie** – Služby skupiny Aruba Group umožňujú zákazníkov pomenovať a klasifikovať aktíva pod ich kontrolou. Príručky zverejnené vo vedomostnej databáze poskytujú presné pokyny, ako tieto operácie vykonávať a aké sú obmedzenia.

Príloha A – ISO 27001:2017 Bezpečnostné aspekty cloudu Aruba Group			
Kontrolovaná oblasť		**Naše kontroly**	**Nástroje a funkcie dostupné pre zákazníkov**
		vymeniť či zlikvidovať, kompletne, v ňom obsiahnuté údaje sa úplne a natrvalo vymažú.	
A.9	**Kontrola prístupu**	**Správa logického prístupu** - Pred prístupom k interným oprávneniam budú pracovníci požiadaní, aby sa identifikovali a overili (prostredníctvom užívateľského mena, hesla a/alebo čipovej karty). Po overení môžu pracovníci Aruba Group pristupovať iba k zdrojom (napr. k systémom, údajom), na ktoré boli výslovne oprávnení, podľa skutočných potrieb pozície, ktorú zastávajú. Užívatelia sú spravovaní prostredníctvom radičov domény Active Directory (AD). Na zaručenie princípu „prerozdeľovania úloh“ je logický prístup do produkčného prostredia riadený prostredníctvom AD na vyhradenej doméne, v rámci ktorej sú užívatelia s rôznymi privilégiami a oprávneniami v súlade s pracovným zameraním danej osoby a dodržiavajú zásady základného práva. Všetci užívatelia sú menovaní jednotlivci, takže neexistujú žiadni skupinoví a/alebo zdieľaní užívatelia a pravidelne podliehajú nezávislému overovaniu bezpečnostným oddelením. **Zásada správy hesiel** – V súlade s bezpečnostnými zásadami skupiny a v súlade s právnymi predpismi o ochrane osobných údajov („minimálne opatrenia“, ustanovenia Úradu na ochranu osobných údajov), sa používajú zásady bezpečnej správy hesiel. Po vytvorení užívateľa je potrebné heslo zmeniť pri prvom prihlásení a potom ho treba pravidelne meniť po definovanom čase.	**Správa logického prístupu** – Zákazník môže kedykoľvek zaregistrovať, upraviť, pozastaviť, znova aktivovať a odstrániť svoje užívateľské profily, ako aj spravovať súvisiace komerčné aspekty (kredity, prahové hodnoty, súvisiace profily atď.). Z hľadiska oprávnení je možné, aby každý zákazník spravoval svoj majetok z administratívneho hľadiska nastavením úrovní zabezpečenia a správou prístupových práv. V závislosti od služby môžu zákazníci najmä: • Priradiť jeden alebo viac virtuálnych počítačov svojim užívateľom, pričom sa spoliehajú na účtovný systém vo virtuálnom počítači. • Pre služby Cloud Object Storage a Cloud Backup je možné vytvoriť jedinečné poverenia, ktoré budú priradené nezávislým pracovným skupinám. • Pre službu Private Cloud je možné v rámci technického ovládacieho panela vytvárať množiny technických užívateľov s rôznymi oprávneniami. • Pre partnerských zákazníkov je vždy možné definovať súbory operácií povolených užívateľom prostredníctvom vhodných pravidiel profilovania. Povolenia sú usporiadané na hierarchickom základe: existujú povolenia „nadradeného“ a „podriadeného“: Povolenie „nadradeného“ automaticky garantuje všetky povolenia „podriadeného“, zatiaľčo povolenie „podriadeného“ garantuje iba seba a môže byť aktivované aj bez povolenia „nadradeného“.
A.10	**Šifrovanie**	**Zabezpečený TLS kanál** – Všetky údaje pochádzajú z/do citlivých systémov analyzovaných systémov, najmä servery vystavené na internete sú chránené bezpečným TLS kanálom pomocou vhodnej konfigurácie na serveroch, aby sa zabezpečilo:	**Kontroly šifrovania** – Odporúčame zákazníkom, aby prijali prístup založený na riziku a zaviedli dodatočné kontroly šifrovania v oblastiach, za ktoré sú zodpovední (pozrite si maticu zodpovednosti) v prípade, že údaje

Príloha A – ISO 27001:2017 Bezpečnostné aspekty cloudu Aruba Group			
Kontrolovaná oblasť		**Naše kontroly**	**Nástroje a funkcie dostupné pre zákazníkov**
		• overenie servera: • šifrovanie relácie pomocou symetrického šifrovacieho algoritmu, ktorý sa považuje za dostatočne bezpečný. Platí to pre toky, ktoré vznikajú interaktívne (prehliadanie webu), ako aj pre toky generované automaticky (napr. dopyt webových služieb). Doteraz sa AES používal hlavne ako symetrický šifrovací algoritmus. Povolená TLS verzia je čo najvyššia, berúc do úvahy možnosti softvérových klientov. Certifikáty SSL servera nainštalované na serveroch vystavených na internete vydáva certifikačný orgán CA, ktorý hlavné prehliadače a operačné systémy považujú za spoľahlivé. Podrobnosti o certifikátoch používaných na cloudových ovládacích paneloch a protokoloch používaných vo verejnej sieti sú k dispozícii v KB na stránke venovanej certifikátom používaným na cloudových ovládacích paneloch. **Šifrovanie údajov v pokoji** – Najvyššie bezpečnostne dôležité údaje „v pokoji“ ako sú heslá, tokeny jednorazového hesla a ďalšie údaje, ktoré musia zostať dôverné, aby sa zabezpečila spoľahlivosť procesov, sa ukladajú pomocou symetrického šifrovania, ktoré sa považuje za dostatočne zabezpečený algoritmus. Pokiaľ ide konkrétnejšiu ochranu prihlasovacích údajov, heslá sú uložené v úložisku v nereverzibilnom „hašovanom“ režime (odtlačok prsta alebo súhrn údajov) pomocou hašovacieho algoritmu SHA-512.	spracúvané v rámci služby Aruba Group sú obzvlášť citlivé. **Cloud Backup – šifrovanie** – Služba Cloud Backup ponúka možnosť šifrovať zálohované dáta ešte pred ich prenosom pomocou silného hesla (AES-256 štandard).
A.11	**Fyzická a environmentálna bezpečnosť**	**Datacentrá** – Systémy na poskytovanie cloudovej služby sa nachádzajú v datacentrách „IT1“ a „IT2“ v Arezzo na Via Gobetti 96 a Via Ramelli 8 a údaje „IT3“ v datacentre v Ponte San Pietro (BG) na Via San Clemente 53. Okrem talianskych datacentier má Aruba Group medzinárodnú sieť infraštruktúry, ktorá je vlastná aj patriaca kvalifikovaným partnerom: • Datacentrum CZ1 v Ktiši v Českej republike, ktoré patrí do medzinárodnej siete datacentier vlastnených organizáciou;	

Príloha A – ISO 27001:2017 Bezpečnostné aspekty cloudu Aruba Group			
Kontrolovaná oblasť		**Naše kontroly**	**Nástroje a funkcie dostupné pre zákazníkov**
		• Datacentrum FR1 v Paríži vo Francúzsku, patriace do siete partnerských datacentier; • Datacentrum DE1 vo Frankfurte v Nemecku, patriace do siete partnerských datacentier; • Datacentrum UK1 v Londýne v Spojenom Kráľovstve, patriace do siete partnerských datacentier; • Datacentrum PL1 vo Varšave, patriace do siete partnerských datacentier. **Budovy odolné voči zemetraseniu** – Datacentrá Aruba Group spĺňajú predpisy o odolnosti voči zemetraseniu. **Kontrola fyzického prístupu** – Vstup do budov je možný len pre tých, ktorí to skutočne potrebujú, po prihlásení sa na recepcii, a prístup do technických miestností je povolený iba oprávneným osobám po identifikácii preukazom a príslušný PINom. Systém kontroly prístupu zahŕňa možnosť povoliť alebo zakázať jednotlivé prístupové karty pre špecifické oblasti, časy a ďalšie kritériá, čo zaručuje úplnú bezpečnosť a jednoduchý prístup. **Systémy proti vniknutiu** – V datacentrách a kanceláriách sú nainštalované padacie mreže, nepriestrelné sklá, pancierové dvere, motorizované brány (pasívne systémy proti vniknutiu) a systémy CCTV a/alebo VMD (aktívne systémy proti vniknutiu). Poplachový systém proti vniknutiu do rôznych zón je plneautomatický. Datacentrá sú rozdelené do niekoľkých zón, ktoré sú monitorované systémami proti narušeniu. Okrem toho sú vo všetkých priestoroch nainštalované pohybové senzory schopné detekovať prítomnosť ľudí; v citlivých priestoroch (datacentrá, rozvodne, sklady) sú aj senzory, ktoré detegujú otváranie dverí a na vstup a výstup sa používa preukaz. **Protipožiarny systém** – Tento systém je navrhnutý tak, aby bol v súlade so zákonom a príslušnými technickými normami. Senzory požiarnej signalizácie sú na všetkých poschodiach budov. **Systém proti vytopeniu** – Sú nainštalované systémy na detekciu úniku vody a proti vytopeniu. Budovy sú tiež umiestnené v rovinatých oblastiach a v zmapovanej polohe vzhľadom na úroveň terénu.	

Príloha A – ISO 27001:2017 Bezpečnostné aspekty cloudu Aruba Group			
Kontrolovaná oblasť		**Naše kontroly**	**Nástroje a funkcie dostupné pre zákazníkov**
		Systém napájania – Tento systém je prítomný v dátových centrách a je nevyhnutný na všetkých úrovniach (napájacie stanice, energetické centrá, UPS, generátory, rozvádzače atď.), aby sa zaručila nepretržitosť napájania za všetkých predvídateľných okolností. Zahŕňa aj vhodné opatrenia na potlačenie vplyvu atmosférických elektrických výbojov, sieťových špičiek atď. **Ventilačný a klimatizačný systém (HVAC)** – Systém je schopný zabezpečiť optimálne klimatické podmienky na bezproblémovú prevádzku serverov hostených v datacentrách. **Internetové pripojenie** – V budovách sa nachádza nevyhnutné pripojenie s kapacitou aspoň dvojnásobkom potrebného minima. **Centrálne operačné stredisko (NOC)** – Datacentrá sú obsluhované 24 hodín denne, 7 dní v týždni, 365 dní v roku, kvalifikovanými systémovými pracovníkmi, čo zaisťuje neustále monitorovanie infraštruktúry, služieb a včasných zásahov v prípade potreby. **Poistenie** – Spoločnosť uzavrela poistnú zmluvu na krytie rizík, ktoré nie sú zmiernené inými bezpečnostnými opatreniami.	

Príloha A – ISO 27001:2017 Bezpečnostné aspekty cloudu Aruba Group			
Kontrolovaná oblasť		**Naše kontroly**	**Nástroje a funkcie dostupné pre zákazníkov**
A.12	**Vybavenie**	**Prevádzkové postupy** – Postupy, ktoré predpisujú prevádzkové správanie, sú zadokumentované, sprístupnené a prijaté príslušným personálom. **Zabezpečenie servera** – Servery, ktoré sú hostiteľmi komponentov kritických pre bezpečnosť služieb podstupujú systémové zásahy určené na zníženie oblasti útoku, ako sú: odstránenie nepotrebného softvéru, deaktivácia nepotrebných služieb/protokolov, inštalácia bezpečnostných záplat odporúčaných predajcami, zavádzanie pravidiel kvôli zložitosti hesiel, povolenie bezpečnostných protokolov atď. **Ochrana DDoS (distribuované odmietnutie služby) –** Je implementovaný systém, ktorý analyzuje prichádzajúce údaje, zisťuje abnormálnu návštevnosť a tam, kde je to možné, blokuje potenciálne nebezpečné balíky. **Protokolovanie** – Protokoly serverov infraštruktúry pre privilegovaný prístup k systémom sa zhromažďujú a uchovávajú v súlade s právnymi požiadavkami. Tieto protokoly pravidelne overuje bezpečnostný tím prostredníctvom interných auditov. Aplikačné denníky operácií vykonávaných počas používania služieb sú sprístupnené zákazníkom. Rovnako aj práca systémových administrátorov podlieha preverovaniu zo strany prevádzkovateľov údajov minimálne raz ročne, aby sa skontrolovalo dodržiavanie organizačných, technických a bezpečnostných opatrení týkajúcich sa spracúvania osobných údajov, ustanovených podľa aktuálnych predpisov. **Monitorovanie a upozornenia** – kritické systémy Služby sú kontrolované systémom nepretržitého monitorovania. Systém má schopnosť generovať „upozornenia“ vo forme e-mailov alebo SMS správ, ktoré vám umožňujú promptne informovať zodpovedný personál o potenciálnej nehode alebo poruche, aby bolo možné čo najskôr vykonať potrebné opatrenia. **Zálohovanie (za ktoré je Aruba Group zodpovedná)** – Funkčné komponenty na poskytovanie služby, spravovanie užívateľov a ďalšie architektonické komponenty služby sa riadia	**Zálohovanie** – Cloudové služby, ktoré ponúka Aruba Group, umožňujú zákazníkom vytvárať a nastavovať vlastné automatizované zálohy prostredníctvom riešení Cloud Backup a Bare Metal Backup, výberom vlastných pravidiel, pokiaľ ide o šifrovanie, frekvenciu, typ (úplné alebo prírastkové) a ďalšie špecifické potreby. Voliteľná funkcia **Disaster Recovery as a Service (DRaaS)** vám tiež umožňuje otestovať postupy núdzového prepnutia bez akýchkoľvek prerušení. Všetky postupy na správu služieb zálohovania a obnovy vykonávajú užívatelia nezávisle a sú popísané v databáze znalostí služby (KB) na vyhradenej stránke, kde sú popísané aj rôzne metódy, ktoré možno použiť na zálohovanie údajov. Nevytvára sa žiadna iná záložná kópia údajov okrem tých, ktoré si nezávisle definujú užívatelia. **Protokolovanie** – Aruba Group poskytuje zákazníkom protokoly aplikácií, ktoré vytvárajú pri používaní služieb. • Cloud PRO: užívateľ si môže zobraziť protokoly operácií na virtuálnych počítačoch, ako je vytváranie, odstraňovanie, ukladanie, obnovovanie, zapínanie, vypínanie, resetovanie, zmena hesiel, zmena funkcií, vytváranie, odstraňovanie a obnovovanie snímok. • Cloud VPS (SMART): užívateľ si môže zobraziť denníky operácií na virtuálnych počítačoch, ako je vytváranie, odstraňovanie, zapínanie, vypínanie, resetovanie a inovácia. • Virtuálne prepínače: užívateľ si môže zobraziť denníky operácií s virtuálnymi prepínačmi, ako je nákup a odstránenie a zmeny funkcií. • Verejné IP adresy: užívateľ si môže zobraziť denníky operácií s verejnými IP adresami, ako je nákup a odstránenie verejnej IP adresy, správa a zmena reverzného DNS.

Príloha A – ISO 27001:2017 Bezpečnostné aspekty cloudu Aruba Group			
Kontrolovaná oblasť		**Naše kontroly**	**Nástroje a funkcie dostupné pre zákazníkov**
		postupmi zálohovania definovanými na úrovni spoločnosti, ktoré sa pravidelne overujú a testujú. **Antivírus** – Všetky zariadenia v sieti skupiny Aruba Group sú kontrolované, monitorované a chránené EDR systémami. EDR technológia (detekcia a odozva koncového bodu) monitoruje známe a neznáme hrozby na všetkých koncových bodoch a firemných serveroch proaktívne a v reálnom čase. Vyhradená skupina s 24-hodinovým pokrytím je zodpovedná za analýzu anomálnych udalostí a rýchle zasahovanie. **Proces správy zraniteľnosti** – Celé okolie Aruba Group je pravidelne kontrolované automatizovanými nástrojmi a kvalifikovanými odborníkmi z odvetvia s cieľom identifikovať akékoľvek možné alebo potenciálne slabé miesta. Každý zistený kritický problém je okamžite nahlásený kompetentnej skupine, čím sa začne cyklus riešenia problému, ktorý môže skončiť novým vydaním alebo zmiernením (napríklad virtuálna oprava). Nakoniec sa na overenie účinnosti vykoná ďalšia kontrola, aby sa zabezpečilo, že sa systém dostal z napadnutia. **Manažment kapacity a riadenie zmien** – Na zabezpečenie riadneho dodávania/poskytovania služby je skupina Aruba Group presvedčená, že je nevyhnutné monitorovať dostupné zdroje, analyzovať kapacity a prijať vhodné opatrenia na ich optimálne využitie a zabezpečiť bežné používanie služieb. Úrovne prepojenia, úrovne obsadzovania zdrojov, miesta na disku a dimenzovanie infraštruktúry sú monitorované špecifickými nástrojmi skupinou operátorov patriacich do centrálneho operačného strediska (NOC), 24/7/365, ktorých úlohou je aj sledovanie akejkoľvek anomálnej udalosti. Monitorovacie nástroje umožňujú nastavenie špecifických kontrol pre každú službu, odhaľujú anomálie a umožňujú predvídať potrebu zmeny. Zmeny, ktoré si vyžiadajú aktivity monitorovania a riadenia kapacít, sú riadené kontrolovaným spôsobom, aby bolo možné overiť výsledky a sledovať vykonávané aktivity. **Aktualizácie a opravy** – Všetky systémy sú pravidelne aktualizované a opravované pomocou centralizovaných nástrojov a podľa interných	• Vyvažovače: užívateľ si môže zobraziť denníky operácií vyvažovača, ako je vytvorenie vyvažovača, úprava vyvažovača, odstránenie vyvažovača, povolenie alebo zakázanie vyvažovača, pridávanie, úprava a odstraňovanie pravidiel. • Jednotné úložisko: užívateľ si môže prezerať denníky operácií na virtuálnych prepínačoch, ako sú nákup a odstránenie a zmeny funkcií. • FTP služba: užívateľ môže zobraziť denníky operácií na FTP účtoch, ako je napríklad aktivácia, odstránenie a úprava priestoru. • Osobný cloud: užívateľ si môže zobraziť denníky operácií na svojom osobnom cloudovom účte, ako je vytváranie, odstraňovanie a zmeny zdrojov. • Cloud Backup: užívateľ si môže zobraziť denníky operácií na svojich zálohovacích účtoch súvisiacich s vytváraním, odstraňovaním a zmenou plánu, zmenou alebo resetovaním hesiel. • Cloudové monitorovanie: užívateľ si môže prezerať denníky operácií svojich monitorovacích služieb a súvisiacich ovládacích prvkov, ako je vytvorenie plánu monitorovania alebo pridanie nového ovládacieho prvku, odstránenie plánu monitorovania alebo kontroly, zmena plánu monitorovania alebo jednoduchú kontrolu. • Cloud Object Storage: užívateľ si môže prezerať denníky operácií na svojich cloudových účtoch úložiska objektov v súvislosti s vytváraním, odstraňovaním a zmenou plánu, zmenou alebo resetovaním hesiel. • Centrum domén: tu si viete zobraziť denníky operácií na vašich doménach a DNS v súvislosti s pridaním novej domény, odstránením domény a zmenami údajov domény, vytvorením DNS, odstránením DNS a zmenami akýchkoľvek DNS záznamov. • Jelastic Cloud: užívateľ si môže zobraziť denníky operácií na svojich účtoch Jelastic Cloud v súvislosti s vytváraním,

Príloha A – ISO 27001:2017 Bezpečnostné aspekty cloudu Aruba Group			
Kontrolovaná oblasť		**Naše kontroly**	**Nástroje a funkcie dostupné pre zákazníkov**
		postupov, ktoré vyžadujú testovanie najskôr vo vývojovom prostredí. Po dokončení tohto kroku sa použijú v produkčnom prostredí. **Synchronizácia** – Všetky cloudové systémy používajú NTP systém na synchronizáciu ich hodín a udržanie konzistencie udalostí. Smerodajným zdrojom synchronizácie hodín je INRiM (http://www.inrim.it). Časové pásmo všetkých používaných systémov je CEST, s výnimkou britského času, kde sa používa GMT. Všetky poskytnuté virtuálne počítače majú časové pásmo založené na CEST a ako zdroj na synchronizáciu hodín používajú hostiteľa, na ktorom sú nainštalované **Multinájom a bezpečné vymazanie údajov– Aruba Group** zaručuje multiprenájmový systém, ktorý umožňuje oddeliť požiadavky jednotlivých zákazníkov od seba a oddeliť požiadavky zákazníkov od požiadaviek poskytovateľa cloudových služieb. Skupina Aruba Group špeciálne vyvinula ovládací panel verejného cloudu ako riešenie pre viacerých nájomníkov v súlade s pokynmi pre bezpečné programovanie a umožňuje iba prístup a kontrolu nad vlastnou cloudovou infraštruktúrou zákazníka. Navyše pri službách PRO, VPS a Private Cloud a pri každom použití externého softvéru je Multinájom garantovaný priamo použitými virtualizačnými systémami. Po uzavretí služby alebo po vyčerpaní kreditu, ako je definované v zmluve, Aruba Group vymaže a natrvalo odstráni údaje z cloudových služieb, ako je popísané na https://kb.cloud.it/account-aru/utilizzo-del-credito/cosa-avviene-ad-esaurimento-del-credito.aspx. V závislosti od služby sa odstránenie môže uskutočniť prostredníctvom API rozhraní, technických ovládacích panelov, skriptov alebo špecifického softvéru. ArubaGroup na správu pravidelného odstraňovania dočasných súborov zo svojich cloudových systémov používa definovaný proces.	odstraňovaním a zmenou plánu, zmenou alebo resetovaním hesiel. • Databáza ako služba (DBaaS): užívateľ si môže prezerať denníky operácií na svojich účtoch „Database as a Service“, ktoré sa týkajú vytvárania, odstraňovania a zmeny plánu, zmeny alebo resetovania hesiel, zálohovania a obnovy databázy a reštartovanie opakovaní. **Správa kapacity** – S ohľadom na riadenie kapacity zákazníkov, Aruba Group umožňuje zákazníkovi neustále monitorovať spotrebu finančných a technických zdrojov, ktoré má k dispozícii, a tiež umožňuje predpovede. Okrem toho sa pri nákupe služby uvádza popis prípadov v ktorých existujú obmedzenia rozšíriteľnosti zdrojov. **Synchronizácia** – Keď sa predpokladá, že synchronizácia hodín môže byť pre zákazníka náročná, podrobné informácie sú uvedené vo verejnej vedomostnej databáze (napríklad na stránke plánovaných operácií) alebo na ovládacích paneloch. **Multinájom** Cloud PRO. Multinájom je garantovaný: • Prostredníctvom ovládacieho panela verejného cloudu špeciálne vyvinutého ako riešenie pre viacerých nájomníkov spoločnosťou Aruba Group a prostredníctvom overených verejných API rozhraní. Tieto riešenia umožňujú iba prístup k vašej cloudovej infraštruktúre a jej spravovanie. • Prostredníctvom virtualizačného systému Hyper-V a VMware. Zákazník má prístup iba ku svojim virtuálnym strojom (VM), ktoré základné hypervízory držia logicky izolované od ostatných. Virtuálne počítače poskytnuté zákazníkovi sa inštalujú s nástrojmi na riadenie prístupu, ktorých prihlasovacie údaje si vyberá priamo zákazník počas vytvárania. Prihlasovacie nástroje, ktoré sa dodávajú so zariadením, sú SSH pre prostredie Linux a RDP pre prostredie Windows. Verejné siete sú zdieľané zákazníkmi, ale

Príloha A – ISO 27001:2017 Bezpečnostné aspekty cloudu Aruba Group			
Kontrolovaná oblasť		**Naše kontroly**	**Nástroje a funkcie dostupné pre zákazníkov**
			na všetkých sprístupnených zariadeniach sa nachádza perimetrický firewall pre zákazníkov. Okrem toho má zákazník možnosť zakúpiť si službu Virtual Switch, ktorá pozostáva z poskytnutia vyhradenej VLAN nezdieľanej s inými zákazníkmi, na ktorú môže zákazník prepojiť príslušné zariadenia kvôli maximálnej segregácii. Cloud VPS (SMART). Multinájom je garantovaný: • Prostredníctvom ovládacieho panela verejného cloudu špeciálne vyvinutého ako riešenie pre viacerých nájomníkov spoločnosťou Aruba Group a prostredníctvom overených verejných API rozhraní. Tieto riešenia umožňujú iba prístup k vašej cloudovej infraštruktúre a jej spravovanie. • Prostredníctvom virtualizačného VMware systému. Zákazník má prístup iba k svojim VM, ktoré základné hypervízory držia logicky izolované od ostatných. Virtuálne počítače poskytnuté zákazníkovi sa inštalujú s nástrojmi na riadenie prístupu, ktorých prihlasovacie údaje si vyberá priamo zákazník počas vytvárania. Prihlasovacie nástroje, ktoré sa dodávajú so zariadením, sú SSH pre prostredie Linux a RDP pre prostredie Windows. Verejné siete sú zdieľané zákazníkmi, ale na všetkých sprístupnených zariadeniach sa nachádza perimetrický firewall pre zákazníkov. Virtual Switch and Hybrid Link: sú to zdroje určené pre jednotlivých nájomníkov. Multinájom je zaručený ovládacím panelom verejného cloudu, ktorý bol špeciálne vyvinutý ako riešenie pre viacerých nájomníkov spoločnosťou Aruba Group a overenými verejnými API rozhraniami. Tieto riešenia umožňujú iba prístup k vašej cloudovej infraštruktúre a jej spravovanie. Súkromný cloud. Multinájom je garantovaný: • Prostredníctvom ovládacieho panela vCloud Director, špeciálne vyvinutého

Príloha A – ISO 27001:2017 Bezpečnostné aspekty cloudu Aruba Group			
Kontrolovaná oblasť		**Naše kontroly**	**Nástroje a funkcie dostupné pre zákazníkov**
			spoločnosťou VMware v režime viacerých nájomníkov. Tento ovládací panel umožňuje prístup iba k vašej cloudovej infraštruktúre a jej spravovaniu. • Prostredníctvom virtualizačného VMware systému. Zákazník má prístup iba k svojmu virtuálnemu dátovému VM centru, ktoré základné hypervízory držia logicky izolované od ostatných. Virtuálne počítače poskytnuté zákazníkovi sa inštalujú s nástrojmi na riadenie prístupu, ktorých prihlasovacie údaje si vyberá priamo zákazník počas vytvárania. Prihlasovacie nástroje, ktoré sa dodávajú so zariadením, sú SSH pre prostredie Linux a RDP pre prostredie Windows. V každom poskytovanom virtuálnom dátovom centre je k dispozícii perimetrický softvérový firewall (NSX Edge), ktorý umožňuje izolovať jeho virtuálne dátové centrum od ostatných a umožňuje zákazníkovi nakonfigurovať optimálne bezpečnostné pravidlá pre príslušné účely. Zákazník má na konfiguráciu vlastnej architektúry možnosť nezávisle si vytvoriť vyhradené privátne siete, ktoré nie sú zdieľané s inými zákazníkmi. V prípade potreby môžu byť verejné siete poskytované aj ako vyhradené siete, ktoré nie sú zdieľané s inými zákazníkmi. Bare Metal Backup. Multinájom je garantovaný: • Prostredníctvom ovládacieho panela verejného cloudu špeciálne vyvinutého ako riešenie pre viacerých nájomníkov spoločnosťou Aruba Group a prostredníctvom overených verejných API rozhraní. Tieto riešenia umožňujú iba prístup k vašej cloudovej infraštruktúre a jej spravovanie. • Pomocou ovládacieho panela Veeam. Zákazníci majú prístup len k svojej vlastnej záložnej množine údajov a nemajú žiadny spôsob ako vidieť alebo ovládať záložné systémy iných zákazníkov.

INTERNET CZ, a. s.
Ktiš 2, 384 03 Ktiš IČO: 26043319 DIČ: CZ26043319
https://www.forpsicloud.cz - https://www.forpsicloud.sk

Príloha A – ISO 27001:2017 Bezpečnostné aspekty cloudu Aruba Group			
Kontrolovaná oblasť		**Naše kontroly**	**Nástroje a funkcie dostupné pre zákazníkov**
			Obnova po havárii Multinájom je garantovaný: • Prostredníctvom ovládacieho panela verejného cloudu špeciálne vyvinutého ako riešenie pre viacerých nájomníkov spoločnosťou Aruba Group a prostredníctvom overených verejných API rozhraní. Tieto riešenia umožňujú iba prístup k vašej cloudovej infraštruktúre a jej spravovanie. • Cez ovládací panel Zerto. Zákazníci majú prístup iba k svojim vlastným súborom údajov a nemajú žiadny spôsob ako vidieť alebo ovládať systémy obnovy po havárii (DR) iných zákazníkov. Zálohovanie na cloude (Evault/Commvault). Multinájom je garantovaný: • Prostredníctvom ovládacieho panela verejného cloudu špeciálne vyvinutého ako riešenie pre viacerých nájomníkov spoločnosťou Aruba Group a prostredníctvom overených verejných API rozhraní. Tieto riešenia umožňujú iba prístup k vašej cloudovej infraštruktúre a jej spravovanie. • Záložným systémom Evault alebo Commvault. Zákazníci majú prístup len k svojej vlastnej záložnej množine údajov a nemajú žiadny spôsob ako vidieť alebo ovládať záložné systémy iných zákazníkov. Monitorovanie cloudu: Multinájom je zaručený ovládacím panelom verejného cloudu, ktorý bol špeciálne vyvinutý ako riešenie pre viacerých nájomníkov spoločnosťou Aruba Group a overenými verejnými API rozhraniami. Tieto riešenia umožňujú iba prístup k vašej cloudovej infraštruktúre a jej spravovanie. Cloudové úložisko objektov: Multinájom je garantovaný: • Prostredníctvom ovládacieho panela verejného cloudu špeciálne vyvinutého ako riešenie pre viacerých nájomníkov spoločnosťou Aruba Group a

Príloha A – ISO 27001:2017 Bezpečnostné aspekty cloudu Aruba Group			
Kontrolovaná oblasť		**Naše kontroly**	**Nástroje a funkcie dostupné pre zákazníkov**
			prostredníctvom overených verejných API rozhraní. Tieto riešenia umožňujú iba prístup k vašej cloudovej infraštruktúre a jej spravovanie. • Systémom Scality Identity and Access Management. Zákazníci majú prístup iba k svojmu vlastnému účtu úložiska a nemajú žiadny spôsob, ako vidieť alebo kontrolovať účty iných zákazníkov. IaaS pre SAP HANA: Multinájom a segregácia sú zaručené vďaka rôznym opatreniam: Prostredníctvom vyhradenej SSL VPN siete, ktorá umožňuje zákazníkovi prístup k systému na správu platformy. Prostredníctvom jedinečného účtu vo virtualizačnom systéme VMware, ktorý umožňuje prístup len k virtuálnym počítačom zákazníka. Prostredníctvom segregácie, ktorú ponúka vyhradená sieť, sprístupnená zákazníkovi a nezdieľaná s inými zákazníkmi. Prostredníctvom interných nástrojov poskytovaných s VM, ktoré umožňujú vytvárať viaceré užívateľské a správcovské profily. Centrum domén: Multinájom je zaručený ovládacím panelom verejného cloudu, ktorý bol špeciálne vyvinutý ako riešenie pre viacerých nájomníkov spoločnosťou Aruba Group a overenými verejnými API rozhraniami. Tieto riešenia umožňujú iba prístup k vašej cloudovej infraštruktúre a jej spravovanie. Jelastic Cloud: Multinájom je zabezpečený dvoma spôsobmi: • Prostredníctvom ovládacieho panela verejného cloudu špeciálne vyvinutého ako riešenie pre viacerých nájomníkov spoločnosťou Aruba Group a prostredníctvom overených verejných API rozhraní. Tieto riešenia umožňujú iba prístup k vašej cloudovej infraštruktúre a jej spravovanie. • Prostredníctvom systému Jelastic: zákazníci majú prístup iba k svojmu Jelastic účtu a nemajú žiadny spôsob, ako vidieť alebo kontrolovať účty iných zákazníkov.

Príloha A – ISO 27001:2017 Bezpečnostné aspekty cloudu Aruba Group			
Kontrolovaná oblasť		**Naše kontroly**	**Nástroje a funkcie dostupné pre zákazníkov**
			Databáza ako služba (DBaaS): Multinájom je zaručený ovládacím panelom verejného cloudu, ktorý bol špeciálne vyvinutý ako riešenie pre viacerých nájomníkov spoločnosťou Aruba Group a overenými verejnými API rozhraniami. Tieto riešenia umožňujú iba prístup k vašej cloudovej infraštruktúre a jej spravovaniu.
A.13	**Bezpečnosť komunikácie**	**Firewall a IPS** – Webové portály poskytované pre služby sú chránené firewallom datového centra cloudových služieb a sú chránené IPS. Čo sa týka výpočtových služieb, všetky virtuálne stroje poskytované spoločnosťou Aruba Group sú modelované a sprístupnené vo forme obrázkov. Tieto obrázky sú vytvárané a testované technikmi Aruba Group a najmä po inštalácii operačného systému a vykonaní prvej konfigurácie je aktivovaný firewallový systém, ktorý poskytuje	**Firewall** – Zákazníci sú správcom svojho vlastného servera a preto majú možnosť meniť nastavenia firewall brány. Sprievodcovia a návody v KB poskytujú informácie o tom, ako oddeliť a chrániť zabezpečenie siete a nastaviť firewall bránu vo vlastnom cloude zákazníka. **Virtuálny prepínač** Zákazníci majú možnosť zakúpiť si službu virtuálneho prepínača, ktorá zahŕňa poskytovanie vyhradenej siete

Príloha A – ISO 27001:2017 Bezpečnostné aspekty cloudu Aruba Group			
Kontrolovaná oblasť		**Naše kontroly**	**Nástroje a funkcie dostupné pre zákazníkov**
		najmenšie možné privilégiá a otvára len nevyhnutné dvere. **Virtuálna súkromná sieť (VPN)** – Vzdialený prístup do firemnej siete (LAN) je udelený iba oprávneným pracovníkom, ktorí takýto prístup vyžadujú; vzdialený prístup je možný iba prostredníctvom VPN siete, ktorá zaisťuje: dôvernosť komunikácie, silné overenie servera a silné (dvojfaktorové) overenie užívateľa.	VLAN, ktorá nie je zdieľaná s inými zákazníkmi, na ktorej zákazníci môžu prepojiť svoje stroje na maximálnu segregáciu s možnosťou nezávisle vytvárať vyhradené súkromné siete, ktoré nezdieľajú iní zákazníci, na konfiguráciu vlastnej architektúry (súkromný cloud). V prípade potreby môžu byť verejné siete poskytované aj ako vyhradené siete, ktoré nie sú zdieľané s inými zákazníkmi. **Geografické umiestnenie údajov na zaručenie bezpečnosti a dodržiavania zásad** – Služby poskytované skupinou Aruba Group možno prípadne aktivovať na základe dátového centra alebo regionálne (čo zodpovedá danej krajine). Zákazníci majú možnosť určiť datacentrum alebo datacentrá, v ktorých budú aktivované ich služby a prenesené ich údaje; pri službách poskytovaných na regionálnej báze majú zákazníci možnosť vybrať si krajinu, v ktorej si službu aktivujú. Skupina Aruba Group za žiadnych okolností nepremiestňuje systémy ani obsah mimo geografických lokalít (datacentier alebo regiónov), ktoré nakonfigurovali jej zákazníci.
A.14	**Akvizícia, vývoj a údržba systémov**	**Spravovanie zmien** – Zmeny v aplikačnom softvéri podliehajú hodnoteniu a schváleniu pred ich zavedením; potom sa testujú pred pokračovaním vo výrobe, aby sa overilo správne zavedenie nových funkcií a absencia regresií. Všetok vyvinutý softvér je navyše spravovaný systémom spravovania verzií.	**Spravovanie zmien** – Skupina Aruba poskytuje zákazníkom denník zmien (ako je popísané na vyhradenej stránke KB), aby ich informovala o vydaniach, opravách, korekciách a aktualizácii služieb.
A.15	**Vzťahy s dodávateľmi**	**Správa dodávateľov** – Skupina Aruba má firemnú politiku, ktorá upravuje vzťahy s dodávateľmi. Politika stanovuje, že pre správnu definíciu a riadenie vzťahov s každým novým dodávateľom je potrebné vždy okrem iného brať do úvahy tieto aspekty, s osobitnou pozornosťou na informačnú bezpečnosť: • hodnotenie rizík a predbežné vyšetrovania, ktoré sa majú vykonať na celkové vyhodnotenie nového dodávateľa;	

Príloha A – ISO 27001:2017 Bezpečnostné aspekty cloudu Aruba Group			
Kontrolovaná oblasť		**Naše kontroly**	**Nástroje a funkcie dostupné pre zákazníkov**
		• výber zmluvných doložiek s cieľom posúdiť, či štandardné zmluvy pokrývajú identifikované riziká, alebo či môže byť potrebné doplniť/zmeniť osobitné doložky; • kontrola prístupu k informáciám, poskytovať prístup dodávateľovi v súlade s princípom „need-to-know“, a teda len k údajom a informáciám, ktoré sú skutočne potrebné a nevyhnutné na výkon príslušných činností; • kontrola prístupu k systémom Aruba Group, ak dodávka umožňuje dodávateľovi prístup k systémom prostredníctvom konkrétnych užívateľov pomocou súkromnej siete (VPN) a špecifického systému odozvy detekcie a infraštruktúry virtuálneho desktopu (VDI), ktorý skupina Aruba Group poskytuje; • monitorovanie neplnenia požiadaviek na pravidelné vykonávanie kontrol za účelom overenia dodržiavania zmluvných požiadaviek dodávateľa a bezpečnosti informácií. Okrem toho externé dodávky potrebné na vývoj, údržbu a poskytovanie služby podliehajú kontrolám, ktorých cieľom je znížiť riziko bezpečnostných incidentov spôsobených nevyhovujúcim materiálom alebo nesprávnym konaním dodávateľov. Všetci poskytovatelia odborných služieb sú povinní podpísať zmluvu o mlčanlivosti (NDA). Zmluvné modely, ktoré používa Aruba Group na poskytovanie služby, umožňujú Aruba Group využívať na vykonávanie svojich činností tretie strany. Táto spolupráca je založená na záväzku skupiny Aruba Group, ktorý je stanovený v zmluvách s akýmikoľvek subdodávateľmi, overiť, či sú na základe typu poskytovanej služby schopní plniť rovnaké požiadavky a úrovne bezpečnosti, ku ktorým sa Aruba Group zaviazala. Aruba Group vedie zoznam subdodávateľov služieb, ktoré sú zákazníkom k dispozícii na požiadanie. Podobne, ak sa prijmú noví/ďalší subdodávatelia, Aruba Group sa zaväzuje informovať svojich zákazníkov v dostatočnom predstihu, aby im umožnila vzniesť námietky alebo odstúpiť.	
A.16	**Spravovanie incidentov zabezpečenia informácií**	**Proces správy incidentov v oblasti bezpečnosti informácií** – Skupina Aruba Group identifikovala a zadokumentovala v rámci špecifickej politiky svoj štruktúrovaný a naprogramovaný prístup k riadeniu	

Príloha A – ISO 27001:2017 Bezpečnostné aspekty cloudu Aruba Group			
Kontrolovaná oblasť		**Naše kontroly**	**Nástroje a funkcie dostupné pre zákazníkov**
		udalostí v oblasti bezpečnosti informácií a incidenty, ktoré sa môžu vyskytnúť v kontexte operácií Aruba Group pri uplatňovaní usmernenia ISO 27035 vo svojom toku riadenia incidentov bezpečnosti informácií. Tento proces sa realizuje prostredníctvom špecifického plánu, ktorý určuje operačné opatrenia, ktoré sa musia zaviesť v prípade incidentov informačnej bezpečnosti. Bol definovaný tok riadenia incidentov a boli identifikované povinnosti súvisiace s jeho uplatňovaním, a to tak z hľadiska riadenia a riešenia incidentov, ako aj z hľadiska strategickej podpory pre včasné prijatie rozhodnutí potrebných na riešenie najrelevantnejších bezpečnostných incidentov (napr. napríklad veľké incidenty, neznáme incidenty, narušenie údajov). Stanovili sa aj časové harmonogramy a postupy na prípravu a doručovanie oznámení týkajúcich sa incidentov informačnej bezpečnosti orgánom, zákazníkom a tretím stranám.	
A.17	**Aspekty zabezpečenia informácií pri riadení kontinuity podnikania**	**Postup riadenia havárií** – **Aruba Group** vypracovala plán kontinuity podnikania a konkrétne postupy týkajúce sa služieb, ktoré sú nevyhnutné na prevádzku datacentier (elektrina, klimatizácia a konektivita). Dátové centrá sú certifikované podľa normy ISO 27001, čo znamená, že všetky infraštruktúry sú chránené opatreniami na zaistenie fyzickej bezpečnosti a kontinuity prevádzky. Dátové centrá Aruba IT1, IT3 DCA a DCB spĺňajú najvyššiu úroveň (Rating 4) podľa normy ANSI TIA 942-B-2017. Táto certifikácia označuje schopnosť zabrániť prerušeniu poskytovania služieb v dôsledku závažných porúch (odolnosť voči výpadkom) a bola dosiahnutá prostredníctvom série návrhových a implementačných opatrení aplikovaných na všetky aspekty výstavby dátového centra: výber lokality, architektonické aspekty, fyzická bezpečnosť, systémy protipožiarnej	**Obnova po havárii ako služba (DRaaS)** – **Aruba Group** poskytuje riešenie na obnovu po havárii ako službu navrhnutú tak, aby firmám zaručila kontinuitu podnikania a umožnila im rýchlo replikovať a obnoviť prístup a funkčnosť pre ich IT infraštruktúru po prerušení v dôsledku kybernetického útoku, zlyhania alebo havarijnej udalosti. Pomocou samoobslužného webového ovládacieho panela so zabezpečeným pripojením môžu zákazníci vytvárať pokyny a zásady obnovy po havárii výberom zdroja (primárna lokalita) a cieľa (sekundárna lokalita) podľa vlastného výberu z vlastnej lokálnej virtuálnej infraštruktúry VMware a Aruba Group datacentier s povolenou službou Private Cloud.

Príloha A – ISO 27001:2017 Bezpečnostné aspekty cloudu Aruba Group			
Kontrolovaná oblasť		**Naše kontroly**	**Nástroje a funkcie dostupné pre zákazníkov**
		ochrany, elektrické systémy, mechanické vybavenie a dátové siete. Dátové centrum s ratingom 4 (predtým Tier 4) ma okrem vyššieho počtu napájacích a chladiacich systémov pre hardvér aj trvalo aktívne redundantné prvky. Na záver možno konštatovať, že dátové centrá sú navrhnuté tak, aby vydržali poruchu v ktorejkoľvek oblasti zariadenia bez prerušenia poskytovaných služieb a sú chránené proti fyzickým rizikám vrátane prírodných katastrof (napr. požiare, záplavy, zemetrasenia atď.). Dátové centrá Aruba IT3 DCA a DCB sú certifikované v súlade s IOS/IEC 22237, medzinárodnou referenčnou normou pre celý životný cyklus dátového centra, od strategickej koncepcie až po realizáciu a prevádzku, v súlade s ANSI/TIA 942 (americká norma) a EN 50600 (európska norma). Cloudové prostredie pozostáva z infraštruktúry väčšieho počtu dátových centier, ktorých služby sú prepojené sieťou IPSEC s vysokou šírkou pásma a nadštandardnou ochranou. Vďaka návrhu štruktúry väčšieho počtu dátových centier je každé dátové centrum prirodzene pripravené na zotavenie po havárii tým, že je logisticky nezávislé od ostatných. Virtualizované servery zákazníkov nepodliehajú geografickému zotaveniu po havárii, pretože zákazníci majú sami k dispozícii všetky potrebné nástroje na vytvorenie vlastných systémov a postupov na zotavenie po havárii na mieru..	
A.18	**Dodržiavanie zásad**	**Ochrana osobných údajov** – Všetky služby sú poskytované plne v súlade s platnými predpismi týkajúcimi sa ochrany osobných údajov v súlade s nariadením (EÚ) 2016/679 („GDPR“), legislatívny dekrét 196/2003 v znení legislatívneho dekrétu 101/2018 a ustanovenia Úradu na ochranu údajov. **Audit** – Udalosti zaznamenané pomocou sledovania, najmä tie, ktoré by mohli naznačovať bezpečnostnú hrozbu, sa pravidelne analyzujú.	

Príloha A – ISO 27001:2017 Bezpečnostné aspekty cloudu Aruba Group			
Kontrolovaná oblasť		**Naše kontroly**	**Nástroje a funkcie dostupné pre zákazníkov**
		Vnútorné kontroly – Manažér auditu a kontroly zabezpečuje aby sa aspoň raz ročne vykonávali kontroly dodržiavania zásad pri poskytovaní cloudových služieb s ustanoveniami tohto dokumentu a platnými predpismi.	

HISTÓRIA VERZIÍ

VERZIA **1.1** K 14/04/2023	***OPIS ZMIEN: Aktualizácie oblastí A.12, A.13, A.17***

VERZIA **1.0** K 01/01/2022	***OPIS ZMIEN: Prvé vydanie***

INTERNET CZ, a. s.
Ktiš 2, 384 03 Ktiš IČO: 26043319 DIČ: CZ26043319
https://www.forpsicloud.cz - https://www.forpsicloud.sk