Cloud forpsi
INTERNET CZ, a.s.

Cloud Security

Příloha A
ISO 27001:2017

14/04/2023

Příloha A - ISO 27001 Bezpečnostní aspekty cloudu skupiny Aruba Group			
Kontrolní oblast		**Naše kontroly**	**Nástroje a funkce, které má k dispozici zákazník**
A.5	**Zásady zabezpečení informací**	**Zásady systému řízení zabezpečení informací (**ISMS) – Skupina Aruba definovala přístup přijatý organizací pro řízení svých cílů v oblasti zabezpečení informací v konkrétních firemních zásadách. Tento dokument byl schválen vedením společnosti a zveřejněn na intranetu společnosti. Na podporu výše uvedených zásad máme další zásady a postupy pro specifické problémy, které definují systém řízení zabezpečení informací skupiny Aruba.	
A.6	**Organizace zabezpečení informací**	**Role a odpovědnosti** – V rámci svých povinností poskytovatele cloudových služeb, jak jsou definovány na modelu sdílené odpovědnosti, určila Skupina Aruba personál, role, dovednosti a odpovědnosti spojené s procesy tak, aby byly v souladu se zásadami rozdělení povinností, nejmenších oprávnění a dvojí kontroly. **Rozdělení povinností (SoD)** – v rámci provozních procesů služeb provádí různé postupy různé osoby, takže žádný člověk nemá kontrolu nad celým procesem. **Nejmenší oprávnění** – Oprávnění k přístupu do prostorů, k zařízením, datům, funkcím apod. se udělují zaměstnancům přiděleným k daným službám v souladu se zásadou „nejmenšího oprávnění“, tedy v rozsahu, který je nezbytný k tomu, aby tyto osoby mohly plnit úkoly, které jim byly přiděleny, ale ne více. **Dvojí kontrola** – Nejkritičtější postupy z hlediska bezpečnosti vyžadují účast nejméně dvou osob.	**Role a odpovědnosti** – obecný popis služby naleznete ve Znalostní bázi na stránce věnované popisu služby spolu se seznamem míst poskytování služby a tabulkou zobrazující model odpovědností sdílených mezi Skupinou Aruba coby poskytovatelem cloudových služeb a jejími zákazníky.
A.7	**Bezpečnost lidských zdrojů**	**Školení personálu** – Servisní personál má odpovídající dovednosti a zkušenosti a má speciální školení pro každou důležitou aktualizaci systému. **Informování** – Zaměstnanci jsou prostřednictvím zvláštních školení pravidelně informováni o otázkách zabezpečení, kyberkriminality obecně a osvědčenými postupy, které je třeba přijmout. **Smlouvy o mlčenlivosti (NDA)** – Nově přijatí zaměstnanci musí podepsat smlouvu o mlčenlivosti, aby ochránili know-how společnosti a další důvěrné informace.	**Školení a informování** – Skupina Aruba disponuje Znalostní bází s informacemi o cloudových službách. Obsahuje informace o službách, návody, tutoriály, dokumentaci k rozhraní pro programování aplikací (API), slovníček pojmů a log změn služeb.
A.8	**Správa aktiv**	**Inventář aktiv** – K dispozici je aktualizovaný inventář aktiv, který zahrnuje záznam virtuálního a	**Vlastnictví aktiv** – V souladu s principem společné odpovědnosti určila Skupina Aruba

Příloha A - ISO 27001 Bezpečnostní aspekty cloudu skupiny Aruba Group			
Kontrolní oblast		**Naše kontroly**	**Nástroje a funkce, které má k dispozici zákazník**
		fyzického vybavení poskytujícího služby a jeho fyzické umístění v rámci infrastruktury Skupiny Aruba. Inventář aktiv se aktualizuje po každé instalaci nového zařízení v infrastruktuře. Kvůli kontrole případných odchylek se navíc denně provádí automatické skenování sítí, aby se zjistil všechen nový majetek. Inventář zahrnuje popis aktiv, ve kterém jsou uvedené související vlastnosti: například typ vybavení (virtuální nebo fyzické), infrastruktura, ke které patří, interní vlastnictví apod. **Nakládání s aktivy** – Existují dále interní postupy, které určují a formalizují činnosti související s přípravou nového vybavení a jeho správou (např. jak provést změnu, jak aktualizovat systémy apod.). **Správa konfigurace** – Seznam komponent systému se pravidelně definuje tak, aby umožňoval identifikaci jednotlivých hardwarových a softwarových komponent a jejich příslušného modelu nebo verze. **Údržba a podpora** – Nejdůležitější hardwarové (HW) komponenty pro plynulost služby jsou ošetřené smlouvami o údržbě, které zaručují opravu nebo výměnu v dostatečně krátkém časovém horizontu dodavatelem, nebo okamžitou skladovou dostupnost identických komponent, které lze v případě potřeby použít. Co se komerčního softwaru (SW) týče, existují příslušné smlouvy o podpoře, které v případě poruch zaručují technickou podporu dodavatele. **Likvidace** – Skupina Aruba zaručuje, že pro likvidaci a zničení již nepoužívaných hardwarových komponent má zvláštní postupy, a to jak pro zahraniční kolokační datacentra, tak pro vlastní datacentra, aby bylo zajištěno, že u každé komponenty s úložištěm, která dosáhla konce své životnosti a musí být zlikvidována a nahrazena, budou všechna v ní obsažená data zcela a trvale odstraněna.	pro každou službu příslušnou zodpovědnost, pokud jde o infrastrukturu, licence, IP adresy, software poskytovaný Skupinou Aruba, software, data a obsah zadaný zákazníkem. Informace o vlastnictví aktiv pro služby jsou zákazníkům k dispozici ve veřejné KB na určené stránce. **Mazání dat** – Pomocí techniky vymazání disku (disk wipe) v cloudovém prostředí má zákazník u služeb VPS (Smart), PRO a Private Cloud možnost trvale vymazat data obsažená v jeho zařízení a znemožnit jejich obnovení. Tento článek v KB obsahuje příslušné kroky. **Označování** – Služby Skupiny Aruba umožňují zákazníkům pojmenovávat a klasifikovat aktiva, která mají pod kontrolou. Návody ve Znalostní bázi poskytují přesné pokyny, jak tyto akce provádět a jaká mají omezení.
A.9	**Kontrola přístupu**	**Řízení logického přístupu** – Před přístupem do interních systémů budou oprávnění pracovníci požádáni o identifikaci a ověření totožnosti (prostřednictvím uživatelského jména, hesla a/nebo čipové karty). Po ověření mohou pracovníci	**Správa logického přístupu** – Zákazník může kdykoli registrovat, upravovat, pozastavovat, znovu aktivovat a mazat své uživatelské profily a spravovat související obchodní aspekty (kredity, stropy,

Příloha A - ISO 27001 Bezpečnostní aspekty cloudu skupiny Aruba Group			
Kontrolní oblast		**Naše kontroly**	**Nástroje a funkce, které má k dispozici zákazník**
		Skupiny Aruba přistupovat jen ke zdrojům (např. systémům, datům), ke kterým mají výslovné oprávnění, a to podle aktuálních potřeb pozice, kterou zastávají. Uživatelé jsou spravováni pomocí kontrolních procesů domény Active Directory (AD). Aby byla zaručena zásada „Rozdělení povinností“, řídí se logický přístup do výrobního prostředí prostřednictvím AD v určené doméně, v jejímž rámci jsou uživatelé s různými oprávněními a privilegii v souladu s pracovní náplní dané osoby a v souladu se zásadou nejmenších oprávnění. Všichni uživatelé jsou jmenované osoby, takže neexistují žádné skupiny a/nebo společní uživatelé. Všichni uživatelé navíc pravidelně podléhají nezávislému ověřování ze strany bezpečnostního oddělení. **Zásady pro správu hesel** – V souladu se zásadami zabezpečení skupiny a v souladu s právními předpisy o ochraně osobních údajů („minimální opatření“, ustanovení Úřadu pro ochranu osobních údajů) se uplatňují zásady bezpečné správy hesel. Po vytvoření nového uživatele se musí heslo změnit při prvním přihlášení a poté musí být pravidelně měněno po uplynutí určené doby.	přidružené profily atd.). Pokud jde o oprávnění, každý zákazník má možnost spravovat svá aktiva z administrativního hlediska, a to nastavením úrovní zabezpečení a správou přístupových práv. V závislosti na službě můžou zákazníci zejména: • Přiřazovat jeden nebo více virtuálních serverů svým uživatelům a spoléhat se přitom na systém účtování ve virtuálním serveru. • Vytvářet pro služby Cloud Object Storage a Cloud Backup jedinečné přístupové údaje, které se budou přiřazovat nezávislým skupinám zdrojů. • Vytvářet sady technických uživatelů s různými oprávněními pro službu Private Cloud v rámci technického ovládacího panelu. • Pro partnerské zákazníky je vždy možné definovat sady aktivit povolených uživatelům, a to prostřednictvím příslušných profilovacích pravidel. Oprávnění jsou uspořádána hierarchicky: Existují „nadřazená“ a „podřízená“ oprávnění. „Nadřazené“ oprávnění automaticky zaručuje všechna „podřízená“ oprávnění, zatímco „podřízené“ oprávnění zaručuje pouze samo sebe. Může ale být aktivováno i bez „nadřazeného“ oprávnění.
A.10	**Šifrování**	**Zabezpečený kanál TLS** – Veškeré datové toky z/do citlivých částí analyzovaných systémů, zejména serverů vystavených na internetu, jsou chráněny zabezpečeným kanálem TLS a pomocí vhodné konfigurace na serverech, aby bylo zajištěno: • ověřování serveru a • šifrování relace pomocí symetrického šifrovacího algoritmu, který je považován za dostatečně bezpečný. To platí jak pro toky vznikající interaktivně (prohlížení webu), tak pro toky generované automaticky (např. dotaz na webové služby).	**Kontroly šifrování** – Doporučujeme, aby zákazníci přijali přístup založený na riziku a zavedli dodatečné kontroly šifrování v oblastech, za které jsou odpovědní (viz Model odpovědnosti), v případě, že jsou data zpracovávaná v rámci služby Skupiny Aruba obzvláště citlivá. **Cloud Backup – šifrování** – Služba Cloud Backup nabízí možnost šifrovat zálohovaná data ještě před jejich přenosem, a to pomocí silného hesla (standard AES-256).

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

Příloha A - ISO 27001 Bezpečnostní aspekty cloudu skupiny Aruba Group			
Kontrolní oblast		**Naše kontroly**	**Nástroje a funkce, které má k dispozici zákazník**
		Jako symetrický šifrovací algoritmus se v současné době používá převážně AES. Povolená verze protokolu TLS je co možná nejvyšší a bere v úvahu možnosti softwarových klientů. Certifikáty SSL Server, které jsou instalované na serverech vystavených na internetu, vydává certifikační autorita, kterou hlavní prohlížeče a operační systémy považují za spolehlivou. Podrobnosti o certifikátech používaných v cloud control panelech a protokolech používaných ve veřejné síti jsou k dispozici v KB na stránce věnované certifikátům používaným v cloud control panelech. **Šifrování dat v klidovém stavu** – Nejkritičtější data „v klidovém stavu“ (jako jsou hesla, tokeny OTP a další data, která musí zůstat důvěrná, aby byla zajištěna spolehlivost procesů) se ukládají pomocí symetrického šifrování s použitím algoritmu, který je považován za dostatečně bezpečný. Pokud jde o ochranu přístupových údajů, ukládají se hesla v úložišti v nereverzibilním šifrovaném režimu (otisk prstu nebo digest dat), a to za využití šifrovacího algoritmu SHA-512.	
A.11	**Fyzické a environmentální zabezpečení**	**Datacentra** – Systémy pro poskytování cloudové služby jsou umístěny v datacentrech „IT1“ a „IT2“ v Itálii v Arezzu na adresách Via Gobetti 96 a Via Ramelli 8 a v datacentru „IT3“ v Ponte San Pietro na adrese Via San Clemente 53. Kromě italských datacenter disponuje Skupina Aruba mezinárodní sítí infrastruktury a to jak vlastní, tak patřící kvalifikovaným partnerům: • Datacentrum CZ1 v Ktiši (Česká republika), které patří do mezinárodní sítě datacenter vlastněných Organizací, • Datacentrum FR1 v Paříži (Francie), které patří do sítě partnerských datacenter, • Datacentrum DE1 ve Frankfurtu (Německo), které patří do sítě partnerských datacenter, • Datacentrum UK1 v Londýně (Spojené království), které patří do sítě partnerských datacenter;	

Příloha A - ISO 27001 Bezpečnostní aspekty cloudu skupiny Aruba Group			
Kontrolní oblast		**Naše kontroly**	**Nástroje a funkce, které má k dispozici zákazník**
		• Datacentrum PL1 ve Varšavě (Polsko), které patří do sítě partnerských datacenter. **Budovy odolné proti zemětřesení** – Datacentra Skupiny Aruba splňují předpisy ohledně odolnosti proti zemětřesení. **Kontrola fyzického přístupu** – Přístup do budov je možný pouze pro ty, kteří ho skutečně potřebují. Po přihlášení na recepci je přístup do technických místností pouze oprávněným pracovníkům po identifikaci elektronickou kartou a příslušným PIN kódem. Systém řízení přístupu zahrnuje možnost povolit a zakázat jednotlivé elektronické karty v konkrétních oblastech, časech a podle dalších kritérií, což zaručuje úplnou bezpečnost a snadný přístup. **Systémy proti vniknutí** – V datacentrech jsou rozmístěné mříže, neprůstřelné sklo, pancéřované dveře a motorizované brány (pasivní systémy obrany proti vniknutí) a instalované systémy bezpečnostních kamer CCTV a VMD (aktivní systémy obrany proti vniknutí). Výstražný systém proti vniknutí do různých zón je plně automatický. Datacentra jsou rozdělená do zón, které jsou monitorovány systémy proti narušení. Kromě toho jsou ve všech prostorách nainstalovány pohybové senzory schopné detekovat přítomnost osob. V citlivých prostorách (datové sály, energetická centra, sklady) jsou také senzory, které detekují otevření dveří. Pro vstup a odchod se používá elektronická karta. **Protipožární systém** – Tento systém je navržen tak, aby vyhovoval zákonu a příslušným technickým normám. Ve všech patrech budov jsou umístěna čidla detekce požáru. **Protipovodňový systém** – V prostorách jsou instalovány systémy detekce kapalin a protipovodňové systémy. Budovy navíc stojí v rovinatých oblastech a ve vyvýšené poloze vzhledem k úrovni terénu. **Energetický systém** – Tento systém je přítomen v datacentrech a je redundantní na všech úrovních (rozvodny, energetická centra, UPS, generátory, rozvaděče atd.), aby byla zaručena plynulost napájení za všech předvídatelných podmínek. Zahrnuje také vhodná opatření k omezení vlivu	

Příloha A - ISO 27001 Bezpečnostní aspekty cloudu skupiny Aruba Group			
Kontrolní oblast		**Naše kontroly**	**Nástroje a funkce, které má k dispozici zákazník**
		atmosférických elektrických výbojů, špiček v síti atd. **Ventilační a klimatizační systém (HVAC)** – Systém je schopen zajistit optimální klimatické podmínky, které vyžaduje bezproblémový provoz serverů umístěných v datacentrech. **Připojení k internetu** – V budovách je k dispozici redundantní připojení s kapacitou alespoň dvakrát vyšší, než je nezbytné minimum. **Síťové operační centrum (NOC)** – Datacentra nonstop obsluhuje kvalifikovaný systémový personál. Díky tomu jsou infrastruktura a služby neustále monitorovány a v případě potřeby dojde k včasnému zásahu. **Pojištění** – Společnost uzavřela pojistnou smlouvu na krytí rizik, která neošetřují jiná bezpečnostní opatření.	

Příloha A - ISO 27001 Bezpečnostní aspekty cloudu skupiny Aruba Group			
Kontrolní oblast		**Naše kontroly**	**Nástroje a funkce, které má k dispozici zákazník**
A.12	**Vybavení**	**Operační procesy** – Tyto postupy předepisují provozní chování a jsou zdokumentovány, zpřístupněny a uznávány příslušnými pracovníky. **Zvyšování odolnosti serverů** – Servery, na kterých jsou umístěny komponenty důležité pro zabezpečení služeb, procházejí systémovými zásahy, které mají omezovat oblast případného útoku. Jde například o odstraňování nepotřebného softwaru, zakazování nepotřebných služeb/protokolů, instalace bezpečnostních balíčků doporučených dodavateli, uplatňování zásad pro složitost hesel, zapínání bezpečnostních logů apod. **Ochrana proti distributed denial-of-service (DDoS) –** Je implementován systém, který analyzuje příchozí data, detekuje abnormální provoz a případně blokuje potenciálně nebezpečné packety. **Logování** – Logy serverů infrastruktury pro privilegovaný přístup k systémům se shromažďují a ukládají v souladu s právními požadavky. Tyto logy pravidelně ověřuje bezpečnostní tým prostřednictvím interních auditů. Logy aplikací o operacích prováděných při využívání služeb jsou zpřístupněny zákazníkům. Ze strany správců údajů rovněž podléhá kontrole činnost správců systému, a to nejméně jednou ročně. Cílem je zkontrolovat dodržování organizačních, technických a bezpečnostních opatření týkajících se zpracování osobních údajů, jak stanovují platné předpisy. **Monitoring a výstrahy** – Kritické systémy služby jsou kontrolovány systémem nepřetržitého monitoringu. Monitoring má možnost generovat „výstrahy“ ve formě e-mailů nebo SMS zpráv, které neprodleně informují odpovědné pracovníky o případné havárii nebo poruše. Díky tomu lze provést potřebná opatření bezprostředně po jejich vzniku. **Zálohování (část, za kterou je zodpovědná Skupina Aruba)** – Funkční komponenty pro poskytování služby, spravování uživatelů a další architektonické složky služby se řídí postupy pro zálohování, které jsou definovány na úrovni společnosti, a které jsou pravidelně ověřovány a testovány. **Antivirová ochrana** – Všechna zařízení v síti Skupiny Aruba jsou kontrolovány, monitorovány a	**Zálohování** – cloudové služby nabízené Skupinou Aruba umožňují zákazníkům vytvářet a nastavovat vlastní automatizované zálohování prostřednictvím služeb Cloud Backup a Bare Metal Backup. Mohou si navíc zvolit i vlastní zásady z hlediska šifrování, frekvence, typu (úplné nebo inkrementální) a dalších specifických potřeb. Volitelná služba **Disaster Recovery as a Service (DRaaS)** dále umožňuje testovat postupy obnovy služeb při selhání bez jakéhokoli přerušení. Veškeré postupy pro správu zálohování a obnovy provádějí uživatelé samostatně. Tyto kroky jsou popsány ve Znalostní bázi služby na příslušné stránce, kde jsou také popsány různé metody, které lze pro zálohování dat použít. Nevytvářejí se žádné jiné záložní kopie dat než ty, které nezávisle definovali uživatelé. **Logování** - Skupina Aruba poskytuje zákazníkům logy aplikací, které se vytvářejí při používání služeb. • Cloud PRO: uživatel může zobrazovat logy operací s virtuálními počítači, jako je vytváření, mazání, ukládání, obnovování, zapínání, vypínání, resetování, změna hesel, změna funkcí, vytváření, odstraňování a obnovování snímků. • Cloud VPS (SMART): uživatel může zobrazovat logy operací s virtuálními počítači, jako je vytváření, mazání, zapínání, vypínání, resetování a aktualizace. • Virtuální switche: uživatel může zobrazovat logy operací s virtuálními switchi, jako je nákup a odebrání a změny funkcí. • Veřejné IP adresy: uživatel může zobrazovat logy operací s veřejnými IP adresami, jako je nákup a odebrání veřejné IP adresy, správa a změna reverzního DNS. • Load balancery: uživatel může zobrazovat logy operací s load balancery,

Příloha A - ISO 27001 Bezpečnostní aspekty cloudu skupiny Aruba Group			
Kontrolní oblast		**Naše kontroly**	**Nástroje a funkce, které má k dispozici zákazník**
		chráněny systémy EDR. Technologie EDR (Endpoint Detection and Response) sleduje známé i neznámé hrozby na všech koncových bodech a firemních serverech v reálném čase i proaktivně. Za analýzu anomálních událostí a okamžitý zásah zodpovídá určená skupina, která pracuje nepřetržitě. **Proces správy zranitelnosti** – Celý perimetr Skupiny Aruba se pravidelně skenuje automatizovanými nástroji a kvalifikovanými odborníky v oboru s cílem rozpoznat všechny možné nebo potenciální zranitelnosti. Jakýkoli zjištěný kritický problém se okamžitě hlásí příslušné skupině. Tím se zahajuje cyklus řešení problému, který může skončit vydáním nové verze nebo zmenšení problému (např. takzvanou virtuální záplatou). Nakonec se pro ověření efektivity provede další skenování, aby se systém ujistil, že se z dané zranitelnosti zotavil. **Řízení kapacit a řízení změn** – Ve snaze zajistit řádné poskytování služeb, považuje Skupina Aruba za nezbytné monitorovat dostupné zdroje, analyzovat kapacity a přijímat vhodná opatření pro jejich optimální využití a zajištění běžného používání služeb. Úroveň konektivity, míra obsazení zdrojů, diskového prostoru a velikost infrastruktury sleduje za využití specifických nástrojů skupina operátorů síťového operačního centra (NOC), a to nonstop. Jejich úkolem je také monitorovat všechny anomální události. Díky monitorovacím nástrojů lze nastavovat specifické kontroly pro každou službu, odhalovat anomálie a předvídat potřeby změn. Ke změnám, které si vyžádalo monitorování a řízení kapacit, se přistupuje kontrolovaným způsobem, aby bylo možné ověřit výsledky a sledovat prováděné činnosti. **Aktualizace a opravy** – Všechny systémy se pravidelně aktualizují a opravují pomocí centralizovaných nástrojů a podle interních postupů, které nejprve vyžadují testování ve vývojových prostředích. Po dokončení této operace se aplikují v prostředí produkce. **Synchronizace** – Všechny cloudové systémy využívají k synchronizaci svého času a udržování konzistence událostí systém NTP. Klíčovým zdrojem pro synchronizaci času je INRiM	jako je vytvoření balanceru, úprava balanceru, odstranění balanceru, povolení nebo zakázání balanceru, přidání, úprava a odstranění pravidel. • Unified Storage: uživatel může zobrazovat logy operací s virtuálními switchi, jako je nákup a odebrání a změny funkcí. • FTP služby: uživatel může zobrazovat logy operací na účtech FTP, jako je aktivace a odebírání a úpravy prostoru. • Private cloud: uživatel může zobrazovat logy operací ve svém privátním cloudu, například vytváření, mazání a změny zdrojů. • Cloud Backup: uživatel může zobrazovat logy operací na svých zálohovacích účtech, které se týkají vytváření, mazání a změny plánu, změny nebo obnovení hesla. • Cloud Monitoring: uživatel může zobrazovat logy operací svých monitorovacích služeb a souvisejících kontrol, jako je vytvoření plánu monitoringu nebo přidání nové kontroly, odstranění plánu monitoringu nebo kontroly, změna plánu monitoringu nebo jednotlivé kontroly. • Cloud Object Storage: uživatel může zobrazovat logy operací na svých účtech úložiště objektů v souvislosti s vytvářením, mazáním a změnou plánu, změnou nebo obnovením hesla. • Domain Center: uživatel může zobrazovat logy operací s doménami a DNS v souvislosti s přidáním nové domény, odstraněním domény a změnami údajů domény, vytvořením DNS, odstraněním DNS a změnami záznamů DNS. • Jelastic Cloud: uživatel může zobrazovat logy operací na svých účtech Jelastic Cloud v souvislosti s vytvářením, mazáním a změnou plánu, změnou nebo resetováním hesel. • Databáze jako služba (DBaaS): uživatel může zobrazovat logy operací na svých účtech „Databáze jako služba“, které se týkají vytváření, mazání a změny plánu,

Příloha A - ISO 27001 Bezpečnostní aspekty cloudu skupiny Aruba Group			
Kontrolní oblast		**Naše kontroly**	**Nástroje a funkce, které má k dispozici zákazník**
		(http://www.inrim.it). Všechny používané systémy pracují v časovém pásmu CEST, s výjimkou Spojeného království, kde se používá GMT. Všechny poskytované virtuální počítače mají časové pásmo na bázi CEST, a jako zdroj pro synchronizaci času používají čas hostu, na kterém jsou nainstalovány. **Multitenant systémy a bezpečné mazání dat**– Skupina Aruba se zaručuje za multitenant systém, který umožňuje oddělit požadavky jednotlivých zákazníků od sebe navzájem a oddělovat požadavky zákazníků od požadavků poskytovatele cloudových služeb. Skupina Aruba vyvinula veřejný cloud control panel jako multitenant řešení v souladu s pokyny pro bezpečné programování a umožňuje přístup a ovládání pouze vlastní cloudové infrastruktury zákazníka. Kromě toho je u služeb PRO, VPS a Private Cloud a při každém použití externího softwaru zaručeno multitenant řešení přímo použitými systémy virtualizace. Po ukončení služby nebo po vyčerpání kreditu, jak je definováno ve smlouvě, Skupina Aruba smaže a trvale odstraní data z cloudových služeb, jak je popsáno na stránce věnované postupu při vyčerpání kreditu. V závislosti na službě může smazání probíhat prostřednictvím rozhraní API, technických control panelů, skriptů nebo specifického softwaru. Skupina Aruba používá definovaný proces pro správu pravidelného mazání dočasných souborů ze svých cloudových systémů.	změny nebo obnovení hesel, zálohování a obnovy databází a restartování instancí. **Řízení kapacit** - Co se řízení kapacit, za které je zodpovědný zákazník, umožňuje Skupina Aruba zákazníkovi neustále sledovat spotřebu finančních a technických zdrojů, které má k dispozici a také předvídat situaci. Kromě toho se při nákupu služby uvádí popis případů, kdy dochází k omezení možností rozšíření zdrojů. **Synchronizace** – Pokud se předpokládá, že synchronizace času může být pro zákazníka obtížná, lze podrobné informace najít ve veřejné Znalostní bázi (například na stránce plánovaných operací) nebo v cloud control panelu. **Multitenant systém** Cloud PRO: Multitenant řešení je zaručeno: • Veřejným cloud control panelem ovládacím vyvinutým Skupinou Aruba jako multitenantní řešení a ověřeným veřejným rozhraním API. Tato řešení umožňují pouze přístup ke cloudové infrastruktuře a její správu. • Virtualizačními systémy Hyper-V a VMware. Zákazník má přístup pouze ke svým virtuálním serverem, které základní hypervizory udržují logicky izolované od ostatních. Virtuální servery poskytnuté zákazníkovi se instalují s nástroji pro řízení přístupu, jejichž přihlašovací údaje si zákazník volí přímo při vytváření. Přihlašovací nástroje, které jsou součástí, jsou SSH pro prostředí Linux a RDP pro prostředí Windows. Veřejné sítě sdílí zákazník, ale na všech poskytnutých zařízeních je k dispozici obvodový firewall, který zákazník používá. Zákazník má navíc možnost zakoupit službu virtuálního switche, která spočívá v poskytnutí vyhrazené sítě VLAN. Ta není sdílena s ostatními zákazníky a zákazník na ní může propojit příslušná zařízení pro maximální oddělení.

Příloha A - ISO 27001 Bezpečnostní aspekty cloudu skupiny Aruba Group			
Kontrolní oblast		**Naše kontroly**	**Nástroje a funkce, které má k dispozici zákazník**
			Cloud VPS (SMART): Multitenant řešení je zaručeno: • Veřejným cloud control panelem vyvinutým Skupinou Aruba jako multitenantní řešení a ověřeným veřejným rozhraním API. Tato řešení umožňují pouze přístup ke cloudové infrastruktuře a její správu. • Virtualizačním systémem VMware. Zákazník má přístup pouze ke svým virtuálním serverům, které základní hypervizory udržují logicky izolované od ostatních. Virtuální servery poskytnuté zákazníkovi se instalují s nástroji pro řízení přístupu, jejichž přihlašovací údaje si zákazník volí přímo při vytváření. Přihlašovací nástroje, které jsou součástí, jsou SSH pro prostředí Linux a RDP pro prostředí Windows. Veřejné sítě sdílí zákazník, ale na všech poskytnutých zařízeních je k dispozici obvodový firewall, který zákazník používá. Virtuální switch a Hybrid Link: jedná se o zdroje vyhrazené jednotlivým účtům. Multitenant řešení je zajištěno veřejným cloud control panelem vyvinutým Skupinou Aruba jako multitenantní řešení a ověřeným veřejným rozhraním API. Tato řešení umožňují pouze přístup ke cloudové infrastruktuře a její správu. Private Cloud: Multitenant řešení je zaručeno: • Control panelem vCloud Director, který speciálně vyvinula společnost VMware v režimu multitenant. Tento control panel umožňuje pouze přístup ke cloudové infrastruktuře a její správu. • Virtualizačním systémem VMware. Zákazník má přístup pouze ke svému virtuálnímu datacentru, které základní hypervizory udržují logicky oddělené od ostatních. Virtuální servery poskytnuté zákazníkovi se instalují s nástroji pro řízení přístupu, jejichž přihlašovací údaje si zákazník volí přímo při vytváření. Přihlašovací nástroje, které jsou součástí, jsou SSH pro prostředí

Příloha A - ISO 27001 Bezpečnostní aspekty cloudu skupiny Aruba Group			
Kontrolní oblast		**Naše kontroly**	**Nástroje a funkce, které má k dispozici zákazník**
			Linux a RDP pro prostředí Windows. V každém virtuálním datacentru je k dispozici softwarový firewall perimetru (NSX Edge), který umožňuje izolovat jeho virtuální datacentrum od ostatních a nakonfigurovat zákazníkovi optimální bezpečnostní pravidla pro dané účely. Zákazník má možnost pro konfiguraci vlastní architektury samostatně vytvářet vyhrazené privátní sítě, které nejsou sdíleny ostatními zákazníky. V případě potřeby je možné veřejné sítě poskytnout i jako vyhrazené sítě, které nejsou sdíleny s jinými zákazníky. Bare Metal Backup: Multitenant řešení je zaručeno: • Veřejným cloud control panelem vyvinutým Skupinou Aruba jako multitenantní řešení a ověřeným veřejným rozhraním API. Tato řešení umožňují pouze přístup ke cloudové infrastruktuře a její správu. • Kontrolním panelem Veeam. Zákazník má přístup pouze ke své vlastní záložní datové sadě a nemá možnost vidět nebo ovládat zálohovací systémy jiných zákazníků. Disaster Recovery: Multitenant řešení je zaručeno: • Veřejným cloud control panelem vyvinutým Skupinou Aruba jako multitenantní řešení a ověřeným veřejným rozhraním API. Tato řešení umožňují pouze přístup ke cloudové infrastruktuře a její správu. • Control panelem Zerto. Zákazníík má přístup pouze ke své vlastní záložní datové sadě a nemá možnost vidět nebo ovládat systémy obnovy po havárii (DR) jiných zákazníků. Cloud Backup (Evault/Commvault): Multitenant řešení je zaručeno: • Veřejným cloud control panelem vyvinutým Skupinou Aruba jako multitenantní řešení a ověřeným

Příloha A - ISO 27001 Bezpečnostní aspekty cloudu skupiny Aruba Group			
Kontrolní oblast		**Naše kontroly**	**Nástroje a funkce, které má k dispozici zákazník**
			veřejným rozhraním API. Tato řešení umožňují pouze přístup ke cloudové infrastruktuře a její správu. • Zálohovacím systémem Evault nebo Commvault. Zákazníci mají přístup pouze ke své vlastní záložní datové sadě a nemají možnost vidět nebo ovládat zálohovací systémy jiných zákazníků. Cloud Monitoring: Multitenant řešení je zajištěno veřejným cloud control panelem vyvinutým Skupinou Aruba jako multitenantní řešení a ověřeným veřejným rozhraním API. Tato řešení umožňují pouze přístup ke cloudové infrastruktuře a její správu. Cloud Object Storage: Multitenant řešení je zaručeno: • Veřejným cloud control panelem vyvinutým Skupinou Aruba jako multitenantní řešení a ověřeným veřejným rozhraním API. Tato řešení umožňují pouze přístup ke cloudové infrastruktuře a její správu. • Systémem Scality Identity a správou přístupu Zákazník má přístup pouze ke svému vlastnímu účtu s úložištěm a nemá možnost vidět ani ovládat účty jiných zákazníků. Domain Center: Multitenant řešení je zajištěno veřejným cloud control panelem vyvinutým Skupinou Aruba jako multitenantní řešení a ověřeným veřejným rozhraním API. Tato řešení umožňují pouze přístup ke cloudové infrastruktuře a její správu. Databáze jako služba (DBaaS): Multitenant řešení je zajištěno veřejným cloud control panelem vyvinutým Skupinou Aruba jako multitenantní řešení a ověřeným veřejným rozhraním API. Tato řešení umožňují pouze přístup ke cloudové infrastruktuře a její správu.
A.13	**Zabezpečení komunikace**	**Firewall a IPS** – Webové portály poskytované službám chrání firewall datacentra cloudové služby a IPS.	**Firewall** – Zákazník je administrátorem vlastního serveru, a proto může měnit nastavení firewallu. Návody a tutoriály v KB poskytují informace o tom, jak oddělit a

Příloha A - ISO 27001 Bezpečnostní aspekty cloudu skupiny Aruba Group			
Kontrolní oblast		**Naše kontroly**	**Nástroje a funkce, které má k dispozici zákazník**
		Co se výpočetních služeb týče, všechny virtuální servery poskytované Skupinou Aruba jsou navrhovány a zpřístupněny ve formě obrazů. Tyto obrazy vytvářejí a testují odborníci Skupiny Aruba a především po instalaci operačního systému a provedení první konfigurace se povoluje systém firewall, který uděluje nejnižší oprávnění a otevírá pouze nezbytné porty. **Virtuální privátní síť (VPN)** – Vzdálený přístup do podnikové sítě (LAN) je umožněn pouze oprávněným osobám, které takový přístup vyžadují. Vzdálený přístup je možný pouze prostřednictvím VPN, která zajišťuje: důvěrnost komunikace, silné ověření serveru a silné (dvoufaktorové) ověření uživatele.	chránit zabezpečení sítě a nastavit firewall ve vlastním cloudu zákazníka. **Virtuální switch** - Zákazník má možnost zakoupit si službu virtuálního switche. Ta zahrnuje poskytnutí vyhrazené sítě VLAN, která není sdílena s ostatními zákazníky a na které mohou zákazníci propojit svá zařízení a získat tak maximální oddělení. Dále nabízí možnost samostatně vytvářet vyhrazené privátní sítě, které nejsou sdíleny ostatními zákazníky, a konfigurovat vlastní architekturu (Private Cloud). V případě potřeby je možné veřejné sítě poskytnout i jako vyhrazené sítě, které nejsou sdíleny s jinými zákazníky. **Geografické umístění dat pro zajištění bezpečnosti a souladu s právními předpisy** - Služby poskytované Skupinou Aruba lze aktivovat podle datacentra nebo regionálně (podle země). Zákazník má možnost specifikovat datacentrum nebo datacentra, ve kterých mají být jeho služby aktivovány a kam mají být jeho data přenesena. V případě služeb poskytovaných na regionální úrovni mají zákazníci možnost vybrat zemi, ve které mají být služby aktivovány. Skupina Aruba v žádném případě nepřesouvá systémy ani obsah mimo geografická umístění (datacentra nebo regiony) nakonfigurovaná zákazníky.
A.14	**Pořízení, vývoj a údržba systémů**	**Řízení změn** – Změny aplikačního softwaru jsou před implementací hodnoceny a schvalovány. Před uvedením na produkci jsou pak testovány, aby se ověřila správná implementace nových funkcí a absence nežádoucích regresí. Navíc je veškerý vyvíjený software řízen systémem verzování.	**Řízení změn** – Skupina Aruba poskytuje zákazníkům seznam změn (jak je popsáno na příslušné stránce v KB), aby je mohla informovat o verzích, opravách a aktualizacích služeb.
A.15	**Vztahy s dodavateli**	**Řízení dodavatelů** - Firemní politika Skupiny Aruba řídí vztahy s dodavateli. Tato politika stanoví, že pro správné určení a řízení vztahů s každým novým dodavatelem je třeba vždy zohlednit mimo jiné následující aspekty. Zvláštní pozornost je pak třeba věnovat bezpečnosti informací:	

Příloha A - ISO 27001 Bezpečnostní aspekty cloudu skupiny Aruba Group			
Kontrolní oblast		**Naše kontroly**	**Nástroje a funkce, které má k dispozici zákazník**
		• Posouzení rizik a předběžná šetření, která mají být provedena za účelem úplného vyhodnocení nového dodavatele. • Výběr smluvních ustanovení, aby se dalo posoudit, jestli standardní smlouvy pokrývají zjištěná rizika, nebo zda je nutné doplnit/změnit konkrétní ustanovení. • Kontrola přístupu k informacím, umožnění přístupu dodavateli v souladu se zásadou „Potřeba vědět“, a to pouze k údajům a informacím, které jsou skutečně potřebné a nezbytné pro výkon příslušných činností. • Správa přístupů k systémům Skupiny Aruba, pokud dodávka umožňuje dodavateli přístup k systémům prostřednictvím konkrétních uživatelů za využití privátní sítě (VPN) a specifické detekční odezvy a systému virtuální desktopové infrastruktury (VDI) poskytnutého Skupinou Aruba. • Monitoring nesrovnalostí, pravidelné provádění kontrol s cílem ověřit, zda dodavatel dodržuje dohodnuté smluvní požadavky a bezpečnost informací. Externí dodávky nezbytné pro vývoj, údržbu a poskytování služeb navíc podléhají kontrolám, jejichž cílem je snížit riziko bezpečnostních incidentů způsobených nevyhovujícím materiálem nebo nesprávným postupem dodavatelů. Všichni dodavatelé profesionálních služeb musí podepsat dohodu o mlčenlivosti (NDA). Smluvní modely používané Skupinou Aruba pro poskytování služeb zajišťují možnost, aby Skupina Aruba využívala k provádění svých činností třetí strany. Tato spolupráce je založena na závazku Skupiny Aruba, který je ve smlouvách s případnými subdodavateli a který zavazuje ověřit, jestli jsou na základě typu poskytované služby schopni splnit stejné požadavky a úrovně bezpečnosti, jak se zavázala Skupina Aruba. Skupina Aruba disponuje seznamem subdodavatelů služeb, který zákazníkům poskytne na vyžádání. Dále se Skupina Aruba zavazuje, že v případě přijetí nových/dalších subdodavatelů bude své zákazníky informovat s dostatečným předstihem, aby případně mohli položit námitky nebo odstoupit od smlouvy.	

Příloha A - ISO 27001 Bezpečnostní aspekty cloudu skupiny Aruba Group			
Kontrolní oblast		**Naše kontroly**	**Nástroje a funkce, které má k dispozici zákazník**
A.16	**Řízení incidentů v oblasti bezpečnosti informací**	**Proces řízení incidentů v oblasti bezpečnosti informací** – Skupina Aruba identifikovala a zdokumentovala v rámci specifických zásad svůj strukturovaný a programový přístup k řízení událostí a incidentů v oblasti bezpečnosti informací, které mohou nastat v souvislosti s činností společností Skupiny Aruba. V rámci řízení incidentů v oblasti bezpečnosti informací uplatňuje postupy dle směrnice ISO 27035. Tento proces se realizuje s využitím zvláštního plánu, který určuje operativní opatření, jež musí být provedena v případě incidentů v oblasti bezpečnosti informací. Skupina určila průběh řízení incidentů a odpovědnosti související s jeho uplatňováním, a to jak z hlediska řízení a řešení incidentů, tak z hlediska strategické podpory pro včasné přijetí rozhodnutí nezbytných pro řešení nejdůležitějších bezpečnostních incidentů (jde například o závažné incidenty, neznámé incidenty a úniky dat). Dále byly definovány časové plány a postupy pro přípravu a doručování zpráv týkajících se incidentů v oblasti bezpečnosti informací úřadům, zákazníkům a třetím stranám.	
A.17	**Aspekty bezpečnosti informací při řízení kontinuity provozu**	**Postup operací při havárií – Skupina Aruba** vypracovala plán kontinuity provozu a konkrétní operace týkající se služeb, které jsou pro provoz datacenter nezbytné (elektřina, klimatizace a připojení). Datacentra jsou certifikována podle normy ISO 27001, což znamená, že všechny infrastruktury jsou chráněny opatřeními k zajištění fyzické bezpečnosti a kontinuity provozu. Datacentra Aruba IT1, IT3 DCA a DCB splňují nejvyšší úroveň (Rating 4) předpisu ANSI TIA 942-B-2017. Tato certifikace označuje schopnost zabránit přerušení poskytování služeb v důsledku závažných poruch (odolnost proti výpadkům) a bylo jí dosaženo řadou návrhových a realizačních opatření aplikovaných na všechny aspekty výstavby datacentra: výběr lokality, architektonické aspekty, fyzické zabezpečení, protipožární systémy,	**Disaster Recovery as a Service (DRaaS)** – Skupina Aruba poskytuje řešení obnovy po havárii jako službu, která má společnostem zaručit plynulost podnikání a umožnit jim rychle replikovat a obnovit přístup a funkčnost jejich IT infrastruktury po přerušení v důsledku kybernetického útoku, selhání nebo katastrofické události. Pomocí samoobslužného webového control panelu se zabezpečeným připojením mohou zákazníci vytvářet pokyny a směrnice pro obnovu po havárii výběrem zdroje (primární umístění) a cíle (sekundární umístění) podle vlastního výběru z virtuální infrastruktury VMware zákazníka a datacenter Skupiny Aruba s aktivovanou službou Private Cloud.

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

Příloha A - ISO 27001 Bezpečnostní aspekty cloudu skupiny Aruba Group			
Kontrolní oblast		**Naše kontroly**	**Nástroje a funkce, které má k dispozici zákazník**
		elektrické systémy, mechanické vybavení a datovou síť. Datacentrum s ratingem 4 (dříve Tier 4) se kromě vyššího počtu napájecích a chladicích systémů pro hardware vyznačuje také trvale aktivními redundantními prvky. Závěrem lze říci, že datacentra jsou navržena tak, aby odolala poruše v jakékoliv oblasti zařízení, aniž by došlo k výpadku poskytovaných služeb, a jsou chráněna proti fyzickým rizikům včetně přírodních katastrof (např. požáry, povodně, zemětřesení atd.). Datacentra Aruba IT3 DCA a DCB jsou certifikována v souladu s IOS/IEC 22237, což je mezinárodní referenční norma pro celý životní cyklus datacentra, od strategické koncepce až po realizaci a provoz, v souladu s předpisy ANSI/TIA 942 (americká norma) a EN 50600 (evropská norma). Cloudové prostředí se skládá z infrastruktury většího počtu datacenter, jejichž služby jsou propojeny sítí IPSEC s vysokou šířkou pásma a nadstandardní ochranou. Díky návrhu struktury většího počtu datacenter je každé z nich nativně připraveno na zotavení po havárii tím, že je z logistického hlediska nezávislé na ostatních. Virtualizované servery zákazníka nepodléhají geografickému zotavení po havárii, protože zákazníci sami mají k dispozici všechny potřebné nástroje k vytvoření vlastních systémů a postupů zotavení po havárii na míru.	
A.18	**Dodržování předpisů**	**Ochrana osobních údajů** – Všechny služby jsou poskytovány v souladu s platnými předpisy o ochraně osobních údajů, v souladu s nařízením (EU) 2016/679 („GDPR“) a ustanoveními Úřadu pro ochranu osobních údajů. **Audity** – Události zaznamenané pomocí sledování, především ty, které by mohly znamenat bezpečnostní hrozbu, se pravidelně analyzují. **Interní kontroly** - Manažer pro audit a kontroly zajišťuje, aby se nejméně jednou ročně prováděly	

Příloha A - ISO 27001 Bezpečnostní aspekty cloudu skupiny Aruba Group			
Kontrolní oblast		**Naše kontroly**	**Nástroje a funkce, které má k dispozici zákazník**
		kontroly souladu cloudové služby s ustanoveními tohoto dokumentu a platnými předpisy.	

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

HISTORIE VERZÍ

VERZE **1.1** K 14/04/2023	***POPIS ZMĚN: Aktualizace oblastí A.12, A.13, A.17***

VERZE **1.0** K 01/01/2022	***POPIS ZMĚN: První vydání***

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