Obchodní společnost: **Domov U Biřičky Hradec Králové**

sídlo: **K Biřičce 1240, 500 08 Hradec Králové**

zastoupená: Ing. Danielou Luskovou, MPA tel.: 495 405 318

IČO: 00579033 , DIČ: CZ00579033

(dále jen ***zákazník***)

a

Obchodní společnost: **PB Com, spol. s r. o.** sídlo: **Zemědělská 898/3, Hradec Králové, PSČ 50003** zastoupená Martinem Říhou, jednatelem

tel.: 495 705 720

IČO: 25280686, DIČ: CZ25280686

zapsána v obchodním rejstříku vedeném Krajským soudem v Hradci Králové, oddílu C, vložce 12553

na straně druhé (dále jen ***servisní organizace***)

ujednali tuto

**SMLOUVU**

**O servisu IT**

**I.**

**Předmět smlouvy**

Předmětem této smlouvy je úprava práv a povinností smluvních stran při zajištění provozu IT zákazníka servisní organizací v provozovnách umístěných v katastru obce Hradec Králové. Servis IT na případných dalších provozovnách zákazníka bude řešen písemným dodatkem k této smlouvě. Hlavním cílem souboru činností prováděných servisní organizací u zákazníka je zajištění bezpečného a plynulého chodu IT bez výpadků, havárií a úniků dat, přičemž bude dbáno na obecná pravidla dodržování kybernetické bezpečnosti tak, jak to vyžaduje současně platná legislativa. Za tímto účelem využívá servisní organizace proaktivní kontinuální monitoring serverů a stanic pro zamezení selhání, kterým lze zabránit prevencí a proaktivním přístupem.

1. Služba **ProactiveMonitoring Plus** zajišťuje průběžné poskytování následujících položek:

* Patch management
* Poskytování helpdesku s garantovanou odezvou
* Offsite záloha dat dle plánu záloh (příloha č.1 této smlouvy)
* Monitoring zálohování včetně testování obnov ze zálohy dle přiloženého harmonogramu
* Monitoring systémových parametrů
* Sledování výkonu
* Monitorování systémových služeb
* Sledování dostupnosti aplikací
* Kontrolu kritických chyb
* Sledování stavu disků
* Garantovanou dobu odezvy technika
* Kvartální vyhodnocení stavu IT infrastruktury – manažerský souhrn

Tato část je službou, o které hovoříme jako o zajištění provozu IT a je z převážné většiny automatizována.

1. **Samostatné služby mimo balíček ProactiveMonitoring Plus:**
	1. **Správa antivirového řešení a poskytování licencí**

Servisní organizace zajišťuje výběr, instalaci, správu a pravidelnou aktualizaci antivirového řešení na koncových zařízeních i serverech zákazníka, včetně poskytování licencí v rozsahu odpovídajícím aktuálnímu počtu zařízení.

* 1. **Poskytování služeb dvoufaktorového ověřování externích uživatelů**

Servisní organizace zajišťuje implementaci a správu dvoufaktorového ověřování pro externí uživatele přistupující do prostředí zákazníka, včetně podpory při aktivaci a správě účtů.

* 1. **Správa prostředí Microsoft Windows a Microsoft 365**

Servisní organizace zajišťuje správu uživatelských účtů, přístupových oprávnění a bezpečnostních politik v prostředí Microsoft Windows Server a Microsoft 365. Tato služba zahrnuje správu licencí, e-mailových účtů, OneDrive, SharePoint a dalších relevantních nástrojů využívaných v rámci Microsoft 365, včetně podpory klientských zařízení s Windows.

1. **Servis IT** (reaktivní podpora a změnové požadavky)

Servisem IT se rozumí činnosti, které souvisí se změnami konfigurace hardware, software a/nebo procesů, ať už v důsledku výpadků nepostižitelných automatizovanými procesy nebo změn, které si vyžádají okolnosti na straně zákazníka (např. růst objemu dat, změna počtu zaměstnanců, zpracovávaných agend apod.). Servis IT bude prioritně vykonáván pomocí vzdálené správy, s výjimkou případů, kdy to není proveditelné nebo praktické, dále viz také článek IV.

**II.**

**Ochrana dat**

Osoby provádějící servis výpočetní techniky zákazníka jsou vázány mlčenlivostí týkající se dat obsažených ve výpočetní technice zákazníka a dále nesmí používat data, výpočetní techniku a programové vybavení zákazníka ve svůj prospěch ani ve prospěch třetích osob. Porušení uvedeného závazku mlčenlivosti či uvedeného zákazu použití dat, výpočetní techniky a programového vybavení se považuje za podstatné porušení smlouvy a zákazník je v takovém případě oprávněn od smlouvy okamžitě písemně odstoupit.

Servisní organizace nenese žádnou odpovědnost za obsah uložených dat, jejich obsah nijak nesleduje a veškerá zodpovědnost za obsah uložených dat je vždy na zákazníkovi. Servisní organizace pro účely této smlouvy rovněž nijak nezodpovídá za zálohování klientských zařízení. Naopak zákazníkovi výslovně doporučuje pravidelné jejich zálohování a periodické kontroly zabezpečení

**III.**

**Hlášení závad**

Zákazník je povinen provádět hlášení závad v pracovní době servisní organizace (Po – Pá, 8:00 – 16:30) výhradně elektronickou formou ve formě vytvoření ticketu na helpdeskovém portálu na adrese: servis.pbcom.cz. Servisní organizace do 15 minut vyrozumí zákazníka prostřednictvím elektronické pošty nebo telefonu o přijetí hlášení o závadě. Pouze v případě závady, která neumožňuje zákazníkovi komunikovat prostřednictvím internetu, nebo pokud zákazník do 20 minut neobdrží vyrozumění o přijetí hlášení o závadě, je zákazník oprávněn provést hlášení závady v pracovní době servisní organizace na servisní telefonní čísla 495 705 720, 732 324 478, 603 152 863 resp. na další telefonní čísla uvedená na http://www.pbcom.cz v sekci Kontakt.

Zákazník je povinen provádět hlášení závad v mimopracovní době servisní organizace výhradně na servisní telefonní čísla 732 324 478, 603 152 863 nebo 603 229 866.

Za zákazníka je oprávněna požádat o servisní zásah pouze osoba pověřená, tato osoba rovněž schvaluje odstranění závady, případně je oprávněna požádat servisní organizaci o placený servisní zásah v případě, že se jedná o práce, které nespadají do rozsahu pokrytého pravidelným měsíčním paušálem. Na žádosti o servisní zásah provedené v rozporu s podmínkami sjednanými v tomto článku smlouvy není servisní organizace povinna brát zřetel, a tudíž není povinna servisní zásah provést.

**Pověřenými osobami jsou:**

* Lukáš Pavel – tel.: 702 124 806
* Daniela Lusková – tel.: 702 088 428
* Zdeněk Fölkl – tel.: 607 210 248
* Michal Souček – tel.: 702 124 802

**IV.**

**Odstranění závad**

Zajištění provozu IT bude probíhat kontinuálně 24/7 s použitím softwarových prostředků zajišťujících Proactive Monitoring u služeb, které jsou poskytovány nepřetržitě (typicky Antivir) a dále v naplánovaných intervalech u služeb, které jsou prováděny v denních či týdenních časových intervalech (typicky kontrola zálohování, patch management).

Servisní zásahy související se zajištěním servisu IT budou zahájeny bez zbytečného odkladu, nejpozději však do čtyř pracovních hodin u zařízení, které vyžadují vysokou dostupnost (servery) a do 24 hodin u ostatních zařízení (stanice, tablety, smartphony, tiskárny). O svátcích a víkendech se doba zahájení servisního zásahu prodlužuje na nejvýše šest hodin s tím, že hlášení závad jsou oprávněné osoby oprávněny provádět pouze v době od 08:00 -16:30. Termíny odstranění závad budou jednotlivě konzultovány s pověřenými osobami v závislosti na charakteru závady (výměna, reinstalace, nahrazení, servis HW v externí organizaci atd.).

Mimo neplánované servisní zásahy bude pracovník servisní organizace navštěvovat provozovnu zákazníka, a to nejméně jednou měsíčně na základě dohody s pověřenými osobami zákazníka. Účelem takových návštěv bude komunikace s jednotlivými uživateli pro odstranění drobných závad, které významně neovlivňují chod IT zákazníka a nebylo k nim vytvořeno samostatné hlášení závady.

**V.**

**Plánované administrativní úkony**

V případě, že zákazník požaduje změnu v nastavení přístupových práv, uložení dalších dat, změny hesel, instalace nových aplikací apod., nepovažuje se takový požadavek za hlášení závady a servisní organizace zajistí provedení patřičných změn do dvou pracovních dnů po obdržení požadavku. Obdobně je potřeba ve lhůtě minimálně dvou pracovních dnů předem hlásit požadavky na součinnost v případě potřeby spolupráce s dalšími subjekty, typicky dodavateli softwarového vybavení, poskytovateli připojení k internetu a podobně. Takovéto požadavky jsou oprávněny vznášet pouze pověřené osoby dle článku III, této smlouvy.

**VI.**

**Součinnost zákazníka k zajištění servisu IT**

Zákazník je povinen poskytnout servisní organizaci fyzický přístup k serveru (serverům) a další infrastruktuře tvořící soubor IT zařízení ve firmě zákazníka, které slouží k ukládání dat v lokální síti, pokud to bude třeba k odstranění závady či běžné údržbě. Zároveň zákazník souhlasí s dálkovým přístupem pověřených pracovníků servisní organizace ke správě serveru (serverů) a stanic nebo jiných koncových zařízení pomocí sítě internet, či jiné sítě pro dálkový přenos dat.

**VII.**

**Finanční odměna a fakturace**

Odměna za služby poskytované v rámci této smlouvy je rozdělena na následující části:

1. Paušální odměna za službu č.1 (Proactive Monitoring Plus) zároveň pokrývající alokaci zdrojů na straně servisní organizace nezbytných k plnění předmětu této smlouvy. Tato služba je fakturována zákazníkovi servisní organizací měsíčně a je stanovena na částku 5.000 Kč měsíčně.
2. Odměna za službu č. 2.1. (Správa antivirového řešení a poskytování licencí), ve výši 50Kč měsíčně za licenci.
3. Odměna za službu č. 2.2. (Poskytování služeb dvoufaktorového ověřování externích uživatelů) ve výši 125Kč měsíčně za každého externího uživatele.
4. Odměna za službu 2.3. (Správa prostředí Microsoft Windows a Microsoft 365)ve výši 100Kč měsíčně za každého uživatele.
5. Odměna za službu č. 3 (Servis IT) bude účtována hodinovou sazbou za práci technika ve výši 1200 Kč za hodinu. Tabulkový soupis provedeného Servisu IT je součástí měsíčního vyúčtování včetně popisu provedených prací a vyčíslení časové náročnosti jednotlivých incidentů.

Zákazník je povinen zaplatit servisní organizaci finanční odměnu vždy souhrnně za 1 kalendářní měsíc na základě faktury-daňového dokladu vystaveného servisní organizací. Servisní organizace vystaví fakturu-daňový doklad a odešle jej zákazníkovi bez zbytečného odkladu po uplynutí příslušného kalendářního měsíce. Doba splatnosti faktury-daňového dokladu (doba splatnosti finanční odměny) je stanovena na 14 dnů ode dne jeho vystavení. Prodlení zákazníka se zaplacením finanční odměny delší než dva měsíce se považuje za podstatné porušení smlouvy a servisní organizace je v takovém případě přerušit poskytování služeb spojených se zajištěním servisu IT. Opětovné zahájení poskytování služeb je podmíněno uhrazením celé dlužné částky.

Všechny ceny uvedené v tomto článku jsou bez DPH.

**VIII.**

**Kontrola a audit dodavatele**

Servisní organizace je povinna umožnit zákazníkovi provádět pravidelné kontroly a audity plnění závazků vyplývajících z této smlouvy, včetně veškerých činností souvisejících s provozem IT infrastruktury. Kontroly budou prováděny po předchozí domluvě v pracovních dnech a časech obvyklých pro činnost servisní organizace. Servisní organizace zajistí přístup k relevantní dokumentaci, systémům a pracovníkům.

**IX.**

**Řetězení dodavatelů**

Servisní organizace se zavazuje nepoužívat subdodavatele pro plnění této smlouvy bez předchozího písemného souhlasu zákazníka. V případě schválení subdodavatele nese servisní organizace odpovědnost za dodržování podmínek této smlouvy subdodavatelem.

**X.**

**Dodržování bezpečnostních politik**

Servisní organizace se zavazuje plně dodržovat bezpečnostní politiky a standardy definované zákazníkem. Zákazník poskytne servisní organizaci znění svých bezpečnostních politik, které jsou pro plnění této smlouvy závazné.

**XI.**

**Řízení změn**

Servisní organizace zavádí formální proces řízení změn, který zajistí koordinaci a dokumentaci všech změn v IT infrastruktuře. Každá změna bude předem schválena zákazníkem a bude zahrnovat možnost návratu do původního stavu (rollback). Primární systém podporující řízení změn je ticketovací systém na adrese servis.pbcom.cz, který má přednastavený typ ticketu pro řízení změn – Žádost o změnu (Change request).

**XII.**

**Kontinuita činností**

Servisní organizace se zavazuje zajistit kontinuitu činností spojených s provozem IT infrastruktury, včetně dodržování SLA. SLA zahrnuje minimální garantovanou dostupnost služeb, reakční doby na incidenty a plány pro obnovu služeb a je stanovena na 98%, počítáno v měsíčních blocích. Servisní organizace poskytne zákazníkovi Disaster Recovery Plan ve formě samostatného dokumentu (příloha č.2 této smlouvy).

**XIII.**

**Informování o incidentech**

Servisní organizace je povinna neprodleně informovat zákazníka o každém zjištěném kybernetickém incidentu, který by mohl ovlivnit poskytované služby. Informování zahrnuje popis incidentu, navržená opatření, harmonogram řešení a závěrečnou zprávu po odstranění incidentu.

**XIV.**

**Profesní pojištění odpovědnosti servisní organizace**

Servisní organizace tímto prohlašuje, že má ke dni uzavření této smlouvy uzavřeno platné pojištění profesní odpovědnosti IT společností u pojišťovny Allianz, dle jejích platných „Zvláštních pojistných podmínek pro pojištění profesní odpovědnosti IT společností“ s limitem pojistného plnění ve výši 2 miliony korun českých. Servisní organizace se zavazuje udržovat toto pojištění platné po celou dobu trvání této servisní smlouvy.

**XV.**

**Smluvní pokuty**

V případě soustavného (tj. více než dvakrát v průběhu jednoho kalendářního měsíce) ne- dodržení termínů započetí servisního zásahu (viz článek IV.) je servisní organizace povinna zaplatit klientovi smluvní pokutu ve výši jednoho celkového měsíčního paušálu.

V případě porušení závazku mlčenlivosti nebo zákazu použití dat (viz článek II) je servisní organizace povinna zaplatit klientovi smluvní pokutu ve výši 100.000,- Kč za každé takové porušení.

V případě prodlení klienta se zaplacením finanční odměny (viz článek VII) je klient povinen zaplatit servisní organizaci smluvní pokutu ve výši 0.05 % z dlužné částky za každý den prodlení.

Uplatní-li smluvní strana právo odstoupit od smlouvy z některého důvodu sjednaného v této smlouvě, není tím dotčeno její právo na zaplacení smluvní pokuty z téhož důvodu.

Všechny ceny uvedené v tomto článku jsou bez DPH.

**XVI.**

**Doba trvání smlouvy**

Tato smlouva se sjednává na dobu neurčitou s účinností od 1. dubna 2025 s výpovědní lhůtou třech (3) měsíců. Výpověď musí mít písemnou formu. Smlouva skončí uplynutím výpovědní lhůty, která počíná běžet prvním dnem kalendářního měsíce následujícího po doručení výpovědi.

Nepodaří-li se poště doručit adresátovi výpověď zaslanou na jeho sídlo zapsané v obchodním rejstříku, považuje se den vrácení nedoručené výpovědi odesílateli za den jejího doručení adresátovi. Stejné platí o doručování odstoupení od smlouvy.

V případě ukončení smlouvy bude ke dni ukončení její platnosti servisní organizací ukončeno poskytování služeb z této smlouvy vyplývající. Servisní organizace poskytne součinnost při předání technologie zvolené nástupnické organizaci případně přímo pracovníkům zákazníka podle článku XVII této smlouvy.

Zákazník se zavazuje, že poskytne servisní organizaci přístup do svých prostor k demontáži serverů a případné ostatní technologie v majetku servisní organizace po ukončení této smlouvy.

**XVII.**

**Předání informací po ukončení smlouvy**

Servisní organizace se zavazuje zahájit proces předání klíčových informací o správě technologie výpočetní techniky klienta nejpozději 15 pracovních dnů před ukončením smlouvy, pokud klient tuto žádost předloží minimálně 20 pracovních dnů před jejím ukončením. Po ukončení smlouvy bude předání pokračovat až do úplného dokončení procesu.

Servisní organizace se zavazuje poskytnout administrátorská hesla, dokumentaci k síťové infrastruktuře, IP adresní plán, přístupová oprávnění a veškeré relevantní konfigurace předem pověřené osobě klienta nebo novému dodavateli IT služeb.

Proces předání musí být zdokumentován a obě strany se zavazují zajistit hladký přechod IT správy, aby nedošlo k narušení provozu organizace.

Za předání informací nutných ke správě technologie výpočetní techniky klienta náleží servisní organizaci základní finanční odměna v částce 12 000,- Kč. Klient je povinen zaplatit servisní organizaci tuto finanční odměnu po předání a podpisu akceptačního protokolu na základě faktury-daňového dokladu vystaveného servisní organizací.

Vyžádá-li si předání informací nutných ke správě technologie výpočetní techniky klienta

dobu delší než 10 hodin, náleží servisní organizaci za její činnost nad tento limit další finanční odměna, která činí částku 1200,- Kč za každou započatou hodinu a poplatek za 1 výjezd technika v částce 250,- Kč, přičemž celková fakturovaná částka za předání IT infrastruktury zákazníka nepřesáhne 24 000,- Kč. Navýšení základní odměny nad 12 000,- je možné pouze po předchozím písemném odsouhlasením ze strany zákazníka.

Všechny ceny uvedené v tomto článku jsou bez DPH.

**XVIII.**

**Závěrečná ustanovení**

Tato smlouva ruší veškeré předchozí smlouvy Zákazníka a Servisní organizace včetně dodatků k nim a tyto nahrazuje touto novou smlouvou. Obě smluvní strany prohlašují, že budou při realizaci této smlouvy dbát na to, aby nebylo poškozeno jejich dobré jméno, a že eventuální spory budou řešit na základě principu dobré vůle a součinnosti. Dohody o doplňcích či změnách této smlouvy musí mít písemnou formu, jinak jsou neplatné. Vztahy vzniklé mezi smluvními stranami při zajišťování provozu IT servisní organizací a zákazníkem, které nejsou touto smlouvou výslovně upraveny, řídí se ustanoveními občanského zákoníku. Obě smluvní strany podpisem této smlouvy stvrzují, že smlouva byla uzavřena z jejich vlastní a svobodné vůle.

V Hradci Králové dne …………….

................................................ ................................................

 zákazník servisní organizace

Příloha č.1

**Plán zálohování**

|  |  |
| --- | --- |
| **Název dokumentu** | **Plán zálohování** |
| **Verze dokumentu** | 2025\_1.0  |
| **Platnost od** | 1.6.2025 |
| **Platnost do** | Do odvolání |
| **Zpracoval** | Robert Houser |
| **Kontroloval** |  Ing. Lukáš Pavel |
| **Schválil** | Ing. Daniela Lusková, MPA, MHA |
| **Datum schválení** | 15.5.2025 |
| **Příští plánovaná revize** | 15.5.2026 |

**1. Jakým způsobem se záloha provádí**

**Interní systémy (Medicus, Sdílené soubory, infrastruktura):**

Zálohování

* Pravidelné zálohy jsou prováděny jednou denně ve 22:00 na úrovni jednotlivých VM. Popis dat umístěných na jednotlivých virtuálních serverech je v bodě 2. tohoto dokumentu. Data jsou ukládána na záložní úložiště Synology, které je umístěno fyzicky mimo primární serverovnu, a po úspěšném dokončení zálohy jsou přenesena do cloudového úložiště PB Com Online Backup přes internet.
* K zálohování se používá software Hornetsecurity VM Backup Unlimited Plus, licencovaný na každý hypervizor (tj. 2 licence). Licence je perpetuální s ročním obnovováním Maintenance.
* Retence záloh:
	+ Lokální úložiště (Synology): 30 dní denních záloh + dlouhodobá archivace dle schématu GFS (Grandfather-Father-Son) uchovávající měsíční zálohy po dobu 1 roku zpětně.
	+ Cloudová záloha (PB Com Online Backup): posledních 14 dní záloh.
* Pravidelné testy obnovy ze záloh probíhají každé čtvrtletí, jejich výsledek je zdokumentován a začleněn do kvartálního reportu.

**Microsoft 365 (E-maily)**

* Microsoft sám data uživatelů nezálohuje, umožňuje pouze obnovu uživatelem náhodně smazaných dat v rámci omezeného období.
* Pokud výchozí obnova dat ze strany uživatelů nestačí, je nutné definovat, které konkrétní účty (vybrané nebo všechny) budou zálohovány externím řešením, včetně způsobu a periodicity těchto záloh.

**2. Umístění zálohovaných dat v interních systémech**

Zálohování interních dat probíhá na úrovni VM pomocí SW Hornetsecurity VM Backup. Tabulka níže obsahuje přiřazení jednotlivých provozovaných aplikací k jednotlivým VM a hypervizorům, na kterých běží.

|  |  |  |  |
| --- | --- | --- | --- |
| **Hypervisor** | **VM** | **Aplikace** | **Poznámka** |
| VMHOST03 | DDSERVER11 | DC, Cygnus 1, Vema | Stará data, pouze pro referenci |
| VMHOST03 | DDSERVER15 | DC, DNS, DHCP, CERT, RADIUS, **Souborový server** | Kromě souborů je zásadní pro ověřování uživatelů a ostatní infrastrukturní záležitosti |
| VMHOST04 | DDSERVER16 | **Medicus**, UniFi, **Cygnus2 - Dochazka** | UniFi kontrolér obsahuje nastavení WiFi pro budovu X |
| VMHOST04 | DDSERVER17 | **Terminál – vzdálený přístup** | Slouží pro vzdálený přístup k aplikacím zvenku |

Příloha č.2

**Disaster Recovery Plan**

|  |  |
| --- | --- |
| **Název dokumentu** | **Disaster Recovery Plan** |
| **Verze dokumentu** | 2025\_1.0  |
| **Platnost od** | 1.6.2025 |
| **Platnost do** | Do odvolání |
| **Zpracoval** | Robert Houser |
| **Kontroloval** | Ing. Lukáš Pavel |
| **Schválil** | Ing. Daniela Lusková, MPA, MHA |
| **Datum schválení** | 15.5.2025 |
| **Příští plánovaná revize** | 15.5.2026 |

1. **Cíle Disaster Recovery Planu**

Hlavním cílem Disaster Recovery Planu (DRP) je zajistit nepřerušené poskytování sociálních a zdravotních služeb v domově pro seniory, a to i v případě závažného selhání IT systémů či jiné mimořádné situace. Důraz je kladen především na ochranu a rychlou obnovu kritických dat a aplikací, jako je lékařský software **Medicus**, který obsahuje citlivé informace nezbytné pro poskytování zdravotní péče klientům.

Cílem je rovněž minimalizace dopadu výpadků IT infrastruktury na každodenní provoz domova, čímž se předejde negativním důsledkům pro klienty a zaměstnance. Rychlá obnova sdílených dokumentů a souborů je nezbytná pro kontinuitu administrativních, organizačních a pečovatelských procesů.

Plán stanovuje jasné požadavky na obnovu systémů tak, aby byly v případě havárie obnoveny v předem definovaných časových rámcích (RTO – Recovery Time Objective) a s co nejnižší ztrátou dat (RPO – Recovery Point Objective). Díky tomu může domov rychle a efektivně reagovat na vzniklou situaci a minimalizovat narušení chodu zařízení, včetně omezení možných dopadů na bezpečnost, zdraví a pohodu klientů.

Disaster Recovery Plan slouží také jako klíčový dokument, který jasně definuje role a odpovědnosti jednotlivých pracovníků v případě incidentu a přispívá k celkové připravenosti organizace na mimořádné situace.

1. **Klíčové systémy a aplikace**

|  |  |  |  |
| --- | --- | --- | --- |
| **Systém / Aplikace** | **Kritičnost** | **Provozováno** | **Poznámka** |
| Medicus (lékařský SW) | Kritické | Interně | Nutná rychlá obnova |
| Sdílené soubory uživatelů | Důležité | Interně | Klíčové dokumenty klientů a provozní dokumentace |
| Microsoft 365 (e-maily) | Důležité | Cloud Microsoft | Důležité pro komunikaci, obnova dle politik MS |
| Cygnus (správa domova) | Kritické | Externě – poskytovatel | Ověřený SLA poskytovatele |
| VEMA (účetnictví, mzdy) | Kritické | Externě – poskytovatel | Ověřený SLA poskytovatele |
| Infrastruktura (AD, DNS, DHCP, CA, RADIUS) | Kritické | Interně | Základní služby ověřování uživatelů |

1. **Analýza rizik a možné hrozby**

Disaster Recovery Planu identifikuje a analyzuje rizika, která by mohla zásadně ohrozit chod organizace, integritu dat nebo kontinuitu poskytovaných sociálních a zdravotních služeb. Mezi hlavní hrozby patří zejména technické poruchy hardwaru, například výpadky serverů či selhání diskových polí, které mohou způsobit nedostupnost klíčových systémů nebo dokonce ztrátu dat.

Velmi častou a statisticky nejvýznamnější příčinou incidentů, které vyžadují obnovu dat, je chyba uživatele. Mezi typické příklady patří neúmyslné smazání důležitých dokumentů nebo nechtěná změna klíčových datových záznamů. Toto riziko vyžaduje nejen technická opatření, jako jsou pravidelné zálohy s dostatečně krátkými intervaly, ale také vzdělávání zaměstnanců a prevenci prostřednictvím odpovídajících uživatelských práv a přístupových politik.

Vážným rizikem jsou také kybernetické incidenty, především ransomwarové útoky, viry či jiné formy škodlivého softwaru. Tyto incidenty mohou vést nejen ke ztrátě přístupu k důležitým systémům, ale také k poškození nebo úniku citlivých osobních údajů klientů a zaměstnanců.

Mezi fyzické hrozby, které by mohly ovlivnit dostupnost IT infrastruktury, patří především požár, záplavy nebo jiné přírodní katastrofy, které mohou způsobit závažné poškození datových center, serveroven či jiných klíčových technických zařízení.

V neposlední řadě je nutné vzít v úvahu také možnost výpadku internetového připojení, což by výrazně zkomplikovalo komunikaci s externími poskytovateli služeb a omezilo dostupnost cloudových aplikací, jako jsou Microsoft 365 nebo externě hostované systémy Cygnus a VEMA.

V plánu je také nutné počítat se selháním externích poskytovatelů služeb, přičemž pro minimalizaci těchto rizik je nezbytné důkladně ověřovat a pravidelně kontrolovat smluvní podmínky (SLA) u všech důležitých partnerů.

Identifikace a pochopení těchto rizik umožňuje organizaci přijmout účinná preventivní opatření a připravit jasné a prověřené postupy pro rychlou a efektivní reakci v případě mimořádných událostí.

1. **Parametry obnovy (RTO / RPO)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Systém / Aplikace** | **RTO (Recovery Time Objective)** | **RPO (Recovery Point Objective)** | **Poznámka** |
| Medicus (lékařský SW) | max. 8 hodin | max. 24 hodin | - |
| Sdílené soubory uživatelů | max. 12 hodin | max. 24 hodin | - |
| Microsoft 365 (e-maily) | max. 12 hodin | dle politik Microsoftu | Dle bodu 6b Smlouvy o poskytování služeb společnosti Microsoft, Microsoft sám data nezálohuje ([odkaz](https://www.microsoft.com/cs-cz/servicesagreement)). |
| Cygnus (správa domova) | dle SLA poskytovatele | dle SLA poskytovatele | - |
| VEMA (účetnictví, mzdy) | dle SLA poskytovatele | dle SLA poskytovatele | - |
| Infrastruktura (AD, DNS, DHCP, CA, RADIUS) | max. 8 hodin | max. 24 hodin | - |

1. **Plán zálohování**

Interní systémy (Medicus, Sdílené soubory, infrastruktura):

**Zálohování**

* Pravidelné zálohy jsou prováděny dle zálohovacího plánu (samostatný dokument). Data jsou ukládána lokálně, a současně do cloudového přes internet.
* Retence záloh:
	+ Lokální úložiště: 30 dní denních záloh + dlouhodobá archivace dle schématu GFS (Grandfather-Father-Son) uchovávající měsíční zálohy po dobu 1 roku zpětně.
	+ Cloudová záloha: posledních 14 dní záloh.
* Pravidelné testy obnovy ze záloh probíhají každé čtvrtletí, jejich výsledek je zdokumentován a začleněn do kvartálního reportu.

**Microsoft 365 (E-maily)**

* Microsoft sám data uživatelů nezálohuje, umožňuje pouze obnovu uživatelem náhodně smazaných dat v rámci omezeného období.
* Pokud výchozí obnova dat ze strany uživatelů nestačí, je nutné definovat, které konkrétní účty (vybrané nebo všechny) budou zálohovány externím řešením, včetně způsobu a periodicity těchto záloh.

**Externí služby**

* Cygnus –dle SLA dodavatele ve smlouvě
* VEMA – dle SLA dodavatele ve smlouvě
1. **Komunikace a eskalační plán**

Kontakty a odpovědné osoby

*IT tým – dodavatel:*

* Primární kontakt je helpdesk dodavatele prostřednictvím e-mailu: **servis@pbcom.cz**
* Pokud povaha závady neumožňuje odeslání e-mailu, kontaktujte telefonicky techniky v tomto pořadí:
	1. Jakub Líbal – tel.: **732 324 478**
	2. Robert Houser – tel.: **603 152 863**
	3. Martin Říha – tel.: **603 229 866**

*Odpovědní pracovníci domova:*

* Lukáš Pavel – tel.: **702 124 806**
* Daniela Lusková – tel.: **702 088 428**

*Externí poskytovatelé:*

* Cygnus (správa domova): Pavel Šrotíř – srotir@iresoft.cz - **733 683 579**
* VEMA (účetnictví, mzdy): **530 500 500**, Daniela Grossová (Cesorg) - daniela.grossova@cesorg.cz - **603 842 207**
1. **Postupy komunikace a schvalování obnovy dat**
2. Pokud plánovaná obnova dat znamená návrat do stavu z minulosti a vede tedy ke ztrátě části dat, musí být o této skutečnosti informováni odpovědní pracovníci domova (Lukáš Pavel nebo Daniela Lusková). Tito pracovníci následně rozhodnou, zda má být obnova provedena.
3. O interní informování zaměstnanců o plánované ztrátě dat rozhodují a provádějí odpovědní pracovníci domova.
4. Pokud při obnově nedochází k významné ztrátě dat (například obnovení jednotlivého souboru nebo menšího množství dat), není nutné další schválení ze strany vedení domova a IT tým dodavatele může obnovu realizovat přímo.
5. **Strategický plán obnovy**

**Obnova v případě bez poruchy hardwaru**

1. V případě, že dojde k nutnosti obnovit data, k jejich znepřístupnění nedošlu z důvodu poruchy hardwaru, tedy zejména (ale nikoliv výhradně) lidskou chybou, chybě softwaru, nebo úmyslným poškozením či kybernetickým útokem, je nutné nejprve vypořádat následující body:
	1. Je třeba určit, zda obnova znamená ještě nějakou další ztrátu dat a zda je tato ztráta akceptovatelná. To musí určit odpovědní zaměstnanci Domova, dle komunikačního plánu popsaného v bodě 7 tohoto dokumentu.
	2. Je třeba rozhodnout, zda je bezpečné provést obnovu na stávající infrastrukturu – to je důležité zejména, pokud je důvodem obnovy úmyslné poškození dat, nebo kybernetický útok. Toto rozhodnutí primárně náleží IT týmu dodavatele.
2. V případě, že se jedná o případ popsaný v b) výše jako úmyslný čin nebo kybernetický útok, je třeba nejprve eliminovat jeho následky a teprve potom provádět obnovu dat, a to i za cenu nedodržení parametrů RTO a RPO.
3. Obnovení malého množství dat (typicky omylem smazané soubory) je možné provést jednotlivě bez další ztráty dat buď operativně pomocí obnovy technologií VSS, nebo Granular restore Hornetsecurity VM Backup.
4. Obnovení většího množství dat, které je typicky spojeno se ztrátou ostatních provázaných dat, je možné až po schválení odpovědnými pracovníky Domova a může být provedeno pomocí technologie Boot from backup nebo VM Restore. Rozhodnutí kterou metodu použít je na IT týmu dodavatele a závisí primárně na možnosti naplnění požadované RPO.

**Náhradní infrastruktura**

* Zákazník využívá dva fyzické servery s technologií Hyper-V. Každý server je samostatně dimenzován pro provoz všech virtuálních strojů zákazníka. V případě poruchy jednoho ze serverů jsou systémy obnoveny na druhý server.
* V případě katastrofického selhání infrastruktury (například požár, záplavy nebo krádež zařízení) bude nutné obnovit data na nově pořízený hardware, případně do cloudového prostředí, podle aktuálních možností zákazníka. V takovém případě, zejména kdyby došlo i ke zničení lokální zálohy, je třeba počítat s tím, že RPO pravděpodobně nebude dodrženo.
* V takovém případě bude priorita následující:
	1. Infrastruktura (zejména AD, DNS, DHCP)
	2. Medicus
	3. Soubory
	4. Ostatní