Bratislavská vodárenská spoločnosť, a.s. Prešovská 48, 826 46 Bratislava 29
zapísaná v Obchodnom registri Mestského súdu Bratislava III oddiel: Sa, vložka č.: 3080/B
IČO: 35850370, DIČ: 2020263432, IČ DPH: SK2020263432

Technická špecifikácia projektu migrácie vybraných služieb, podnikových procesov a dát na Microsoft 365

Zámerom obstarávateľa Bratislavská vodárenská spoločnosť, a.s. (**BVS** alebo **Obstarávateľ**) je zabezpečiť migráciu vybratých služieb z existujúceho on-premise prostredia na riešenie Microsoft 365 (**M365**) vrátane modernizácie používateľského prostredia, zabezpečenia procesov súvisiacich s migráciou a integráciou vybraných dát s existujúcimi onpremise systémami.

Základné informácie o Obstarávateľovi v kontexte zákazky:
Bratislavská vodárenská spoločnosť, a.s. je zaradená do sektoru s vysokou úrovňou kritickosti – voda a atmosféra:

- Je potrebné zohľadniť požiadavky zákona o č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, v znení neskorších predpisov a Vyhlášky Národného bezpečnostného úradu č. 362/2018 Z.z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení;
- Obstarávateľ má povinnosť postupovať podľa zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov, v znení neskorších predpisov;
- Aktuálny počet zamestnancov BVS je 1200, z ktorých je:
- 50 zamestnancov IT/Security (užívatelia pristupujúci k informačným systémom v špeciálnom/chránenom režime);
- 710 administratíva / riadiaci pracovníci v teréne (užívatelia pristupujúci k informačným systémom v štandardnom režime);
- 440 pracovníkov v teréne (užívatelia nepristupujúci k informačným systémom, alebo užívatelia s obmedzeným prístupom k informačným systémom);
- Obstarávateľ identifikuje značnú mieru rezistencie na zmenu. Úspešná implementácia a efektívne využitie M365 aplikácií z užívateľskej perspektívy bude vyžadovať zo strany úspešného uchádzača efektívnu a rozsiahlu M365 adopčnú a školiacu kampaň za zohľadnenia identifikovaného stavu na základe auditu u Obstarávateľa.

Analýza, migrácia, implementácia a podpora (*support*) pri prechode na služby Microsoft 365

1. Popis „AS IS“ a „TO BE“ stavu

	OBLASŤ	AS IS stav	TO BE stav / minimálne požiadavky
1	**Licencovanie**	Aktuálne využívané: • Office 2016 – 900 licencii • Office 365 Business Basic - 80 licencií • Teams – 80 licencií • SharePoint 2013 – 900 licencií	Nastavenie novej licenčnej politiky: • Funkčne a nákladovo optimálna kombinácia M365 licencií definovaná na základe výstupov analýzy o Prehľad jednotkových cenníkových cien, alebo odporúčaných koncových cien vybraných licencií Microsoft, na vyžiadanie Obstarávateľa, najviac však 1xmesačne počas poskytovania služieb o Optimalizácia a vyhodnocovanie využívania licenčných balíkov M365 počas poskytovania služieb, najviac však 1x12 mesiacov
2	**Active Directory**	*Active Directory* („**AD**“)[1] v on-premise (aj zostáva): • Centralizovaný AD s hybridnou prípravou cez federáciu • Doménové GPO pre užívateľov a zariadenia • Väčšina aplikácií integrovaných s AD a využívajúcich aj SSO • Oddelené OU pre užívateľské účty • UPN nie je mailová adresa • Neexistuje centralizovaná politika pre cloud-ready identity	Požiadavky na integráciu: • Integrácia AD v hybridnom režime • Redizajn Microsoft Entra Connect. • Zabezpečenie, že privilegované identity sa nebudú synchronizovať medzi cloudovými a on-premise prostredím • Návrh a realizácia IAM, RBAC • Multifactor • Zachovanie SSO pre aplikácie Obstarávateľa v AS-IS stave • Príprava na hybridné identity (SSO, MFA) • Prípadné odporúčania reorganizácie organizačných jednotiek („**OU**“) Obstarávateľa so zreteľom na bezpečnostné štandardy Obstarávateľa

[1] Zoznam všetkých skratiek použitých v dokumente sa nachádza na stranách 25-26.

3	**Servery**	Exchange v on-premise: • Exchange 2016 – 2 servery v DAG konfigurácii • On-premisové mail security, IPS/IDS a WAF • SharePoint 2013 – 1 aplikačný, 1 databázový server • SharePoint 2013 - iba pre on-premise prostredie	Požiadavky na integráciu: • Migrácia on-premise Exchange (výber hybridnom režime s Exchange SE, staged migrácia) do • Exchange Online - migrácia užívateľských mailboxov • Exchange SE - migrácia systémových mailboxov • Zabezpečenie minimálne tej istej úrovne mail security ako s onpremisovými riešeniami • Migrácia SharePointu do SharePoint Online
4	Security	Aktuálne využívané: • Používané autentifikačné protokoly sú Kerberos a časti NTLMv2 • SSO pre väčšinu aplikácií • Neexistuje MFA, žiadna integrácia s cloudovým zabezpečením. • Antivírus tretích strán, žiadne Microsoft Defender riešenia.	Požiadavky na integráciu: • V prípade nemožnosti používať Kerberos a NTLMv2 plná súčinnosť pri zmene autentifikačného protokolu OAuth pre on-premisové aplikácie • Implementácia Microsoft Defender for Endpoint ako náhrada pre antivírus tretích strán s EDR funkcionalitou • Aktivácia MFA, Conditional Access Policies • Návrh riešenia na nasadenie DLP v rozsahu navrhnutých licencií podľa interných politík Obstarávateľa • Nasadenie Microsoft Purview eDiscovery solutions • Podrobný monitoring a audit systémov • Školenie IT tímu pre správu bezpečnostných politík • Príprava a implementácia Mobile Device Management (MDM) • Vybudovanie centrálneho logovacieho riešenia na platforme Log analytics pre zabezpečenie retencie auditnej stopy na 12 mesiacov. Riešenie musí obsahovať celú auditnú stopu, ktorú budú generovať všetci zamestnanci BVS, externisti a využívané služby M365.

5	**Sharepoint**	Verzia SharePoint 2013: • Využitie ako úložisko, intranetové tímové lokality, sharepoint listy, žiadne workflows nie sú využívané • využívaný pre internú spoluprácu a dokumentáciu. • Cca 800 používateľov, 50 aktívnych knižníc, 10 lokalít. • Existencia 4 dorobených aplikácií	Odstavenie on-premise SharePoint 2013: • Migrácia všetkých lokalít a dokumentov do SharePoint Online • Náhrada InfoPath riešení modernými Power Apps. • Vytvorenie šablón pre tímové stránky • Sharepoint Online, báza pre DMS, PowerApps, Workflows formou služieb na vyžiadanie v prípade potreby riešenia komplexných nových požiadaviek Obstarávateľa, ktoré neboli súčasťou "as is stavu"
6	**Integrácie**	AD & SAP, GIS (Geograficky informačný systém), eHuman (HR system), CDesk (It ticketing system), Registratúra (Memphis), DMS systém, eGOV (eSlovensko)	• Zmapovanie integračných bodov. • Migrácia alebo redizajn integrácií do Power Platform. Prepojenie so SAP, GIS, atď. ak je potrebné cez Power Automate alebo API
7	**Zálohovanie**	Zálohovanie on-premisového Exchange a SharePointu: • Zálohovanie je zabezpečené prostredníctvom on-premisového zálohovacieho nástroja • Onprem zálohovacie prostredie nemá možnosť zálohovania cloudových riešení • On-premisové zálohovacie médium nie je kompatibilné na ukladanie M365-kových záloh	**Zálohovanie cloudových služieb:** Zabezpečenie záloh dát z Exchange online, Sharepoint online a OneDrive v rámci: • Microsoft zálohovanie v rámci M365 licencií, odhadovaná veľkosť zálohovania je 10TB v prvom roku • „M365 Backup" add-on, alebo pomocou iného adekvátneho riešenia. Azure subskripcia – kredit bude predplatený Obstarávateľom na základe potreby a nie je predmetom tejto špecifikácie • Azure files – sync do lokálneho servera Výsledkom návrhu „to be" stavu je návrh ukladania záloh aj mimo dátových centier Microsoft-u, ale na území EU z dôvodu zabezpečenia GDPR
8	**Komunikácia**	Primárne komunikačné nástroje: • Outlook 2016 + Exchange 2016 • Teams (80 licencií), Skype for Business • VoIP • Mobilné telefóny	Zmena vo využívaní komunikačných nástrojov: • Zrušenie Skype for Business • Minimalizácia využívania VoIP • Nasadenie Microsoft Teams ako primárneho interného komunikačného nástroja Zaškolenie používateľov

9	**Operačné systémy a Office**	Aktuálny stav OS: • Microsoft Windows 10 (Enterprise LTSC a Pro): 537 • Microsoft Windows 11: 193 Office: • Microsoft Office Standard 2016: 730	Špecifikácia podmienok pre inštaláciu offline Office balík-u na všetky koncové stanice pre: • užívateľov pristupujúcich k informačným systémom v špeciálnom/chránenom režime (50) užívateľov pristupujúcich k informačným systémom v štandardnom režime (1250) Upgrade OS z Win10 na Win11 nie je predmetom dodavky
10	**PC hardware**	Nie je súčasťou zákazky	Nie je súčasťou zákazky
11	**Mobilné zariadenia**	Aktuálny stav OS: • Android • iOS	Nasadanie MDM (Intune) pre mobilné zariadenia a NB/PC/tablety: • užívateľov pristupujúcich k informačným systémom v špeciálnom/chránenom režime (50) • užívateľov pristupujúcich k informačným systémom v štandardnom režime (810) • užívatelia nepristupujúci k informačným systémom, alebo užívatelia s obmedzeným prístupom k informačným systémom (440)
12	**Support**	Podpora pre on- premisové prostredie: • Interný IT tím • Externý - N/A	Podpora pre cloudové/hybridné prostredie: • Vytvorenie dokumentácie pre 1. a 2. úroveň podpory • Školenie interného IT oddelenia • Definovaná SLA pre postimplementačnú podporu • Požadovaný HyperCare 24/7 po dobu tri mesiace po ukončení migrácie

2. Predmet zákazky

Predmetom zákazky sú jednotlivé fázy súvisiace s priamym dopadom na migráciu a prevádzku služieb M365:

1. **Analýza východiskového stavu (AS-IS) IT prostredia spoločnosti**
   a. Analýza infraštruktúry priamo súvisiacej s migráciou na M365 v organizácii Obstarávateľa
   b. Identifikácia závislostí, rizík a integrácií spojených so stavom AS-IS

2. **Návrh budúceho stavu (TO-BE)**
   a. Návrh licenčného modelu s potrebným počtom typových licencií a následná súčinnosť pri nákupe licencií
   b. Návrh architektúry a technických komponentov priamo súvisiacich s predmetom zákazky
   c. Návrh optimalizácie procesov a nákladov súvisiacich s použitím balíka služieb Microsoft 365
   d. Požiadavky na Hardvér /Softvér súvisiacich s nasadením a použitím balíka služieb Microsoft 365
   e. Návrh kapacity siete a zálohovania súvisiacich s nasadením a použitím balíka služieb Microsoft 365
   f. Časový harmonogram a odporúčanie načasovania nákupu jednotlivých licencií za účelom maximalizácie efektivity ich využitia

3. **Príprava detailného časového plánu dodávky predmetu zákazky spolu s definovanými míľnikmi**
   a. Definovanie fáz, kľúčových míľnikov, prechodových období
   b. Harmonogram s definovanými termínmi a míľnikmi

4. **Implementácia, systémové integrácie**
   a. Nasadenie Microsoft 365 služieb
      i. Migrácia dát (pošta, dokumenty, SharePoint, a ostatné zložky určené na migráciu spojené s nasadením Microsoft 365 služieb)
      ii. Nastavenie zabezpečenia, compliance a governance
   b. Hypercare – po dobu 3 mesiacov po protokolárnom prevzatí diela časti migrácie na Microsoft 365 v režime 24/7

Súčasťou implementačnej a systémovej integrácie sú aj nasledujúce aktivity:

- Tenant Security Hardening (stanovenie perimetra bezpečnosti Cloudových služieb ako sú Identita, Elektronická pošta, Správa koncových staníc, Microsoft Teams, Microsoft Sharepoint, Microsoft OneDrive, Power Platform, Bezpečnosť, Monitoring, Microsoft Azure, a to v súlade so štandardami aplikovateľnými pre

cloudové služby a hybridnú infraštruktúru podľa CIS, ISO 27001, NIS2 a iných záväzných právnych predpisov na úseku kybernetickej bezpečnosti.)

- Implementácia Cloud Adoption Framework Enterprise Scale Landing zónu v súlade s klasifikáciou definovanou MIRRI SRv kategóriách U1-U3
- Návrh matice prístupov
- Adopčná kampaň - príprava návrhov, metodík, realizácia, vyhodnotenie

5. Školenia zamestnancov

a. IT admin školenia / workshopy
b. „*Train the trainer*“ školenia / workshopy
c. Koncoví používatelia - e-learning: základné a pokročilé školenia

6. Dokumentácia

a. poskytnutie technickej, systémovej, administrátorskej, užívateľskej dokumentácie záznamy o konfiguráciách

7. Technická podpora

a. Štandardná reaktívna podpora - SLA pre prípad incidentov
b. Proaktívna podpora 8 Osobohodín za mesiac počas 24 mesiacov po ukončení Fázy 4b: Hypercare.
c. Nadštandardná podpora – v zmysle schválených zmenových požiadaviek

2.1 Analýza východiskového stavu (AS-IS) IT prostredia spoločnosti

Analýza infraštruktúry priamo súvisiacej s migráciou na M365 (minimálne v rozsahu):

- Posúdenie aktuálneho stavu.
- Návrh prípadných zmien v rámci infraštruktúry potrebných na úspešnú implementáciu.

Audit existujúcich licencií minimálne v rozsahu:

- Identifikácia počtu a typov Obstarávateľom zakúpených licencií a do akej miery sú využívané.
- Nevyužité licencie a príčiny ich nevyužitia. Identifikácia licencií, ktoré sa aktuálne nevyužívajú.
- Kompatibilita licencií. Overenia, či sú existujúce licencie kompatibilné s plánovanými službami.
- Iné úkony (resp. podľa *best practice* Zhotoviteľa), ktoré sú potrebné na úspešné vykonanie auditu za účelom získania informácií pre nasledujúce postupy.

Analýza on-premisového AD prostredia minimálne v rozsahu

- Počet a typ objektov v AD (používatelia, skupiny, počítače).
- Existujúce GPO a ich kompatibilita s Azure AD.
- Stavu DNS, sieťových konfigurácií a autentifikácie.

- Kompatibilita existujúcich aplikácií a služieb s Azure AD.
- Identifikácia aplikácií využívajúcich Kerberos a NTLMv2.
- Overenie DNS záznamov a názvov domén.
- Overenie aktuálnych nastavení Microsoft Entra Connect.
- Analýza nastavenia možnosti použitia Password Hash Synchronization alebo Passthrough Authentication.
- Iné úkony (resp. podľa *best practice* Zhotoviteľa), ktoré sú potrebné na úspešné vykonanie analýzy on-premisového AD prostredia.

Analýza on-premisového Exchange prostredia minimálne v rozsahu:

- Exchange verzia: Overenie aktuálnej verzie Exchange servera.
- Overenie systémových požiadaviek pre hybridnú migráciu.
- Overenie dostupnosti dostatočného diskového priestoru.
- Počet mailboxov: Zistenie počtu aktívnych mailboxov a ich celkovej veľkosti.
- Distribučné skupiny: Identifikovať všetky používané distribučné skupiny, ktoré je potrebné migrovať.
- Verejné priečinky: Skontrolovať, či sú používané verejné priečinky, a zmapovať ich obsah.
- Archívy: Určiť, či sú mailboxy archivované lokálne alebo na serveri.
- Overenie, záloh Exchange databáz, vrátane nastavení. Overenie integrity záloh testovacou obnovou.
- Identifikácia všetkých používaných certifikátov SSL/TLS.
- Identifikácia všetkých certifikátov s dostatočnou platnosťou na pokrytie migrácie. Overenie, či certifikáty zahŕňajú všetky potrebné záznamy (napr. autodiscover, mail, atď.).
- Overenie dostupnosti a stability internetového pripojenia. Do analýzy je potrebné zahrnúť aj branch office-y Obstarávateľa. Rýchlosti internetového pripojenia na lokalitách Obstarávateľa budú poskytnuté v čase vykonávania analýzy.Kontrola aktuálneho nastavenia DNS pre autodiscover, MX a SPF záznamov.
- Kontrola firewall-ov pre pripojenia služby Microsoft.
- Kontrola toku pošty: smerovanie správ, Hygiena pošty, On-premise Mailové služby (Exchange server, SMTP Relay), Zdroje SMTP preposielania (Multifunkčné zariadenia, Aplikácie).
- Povolenia na úrovni poštovej schránky (Shared mailbox, Delegation).
- Analýza záloh všetkých mailboxov a databáz pred migráciou.
- Iné úkony (resp. podľa best practice Zhotoviteľa), ktoré sú potrebné na úspešné vykonanie analýzy on-premisového Exchange prostredia.

Analýza on-premisového SharePoint prostredia minimálne v rozsahu:

- Overenie aktuálnej verzie aplikačného a databázového servera.
- Overenie systémových požiadaviek, napr. dostupnosti dostatočného diskového priestoru a veľkosť databáz.
- Overenie, webových aplikácií a kolekcie lokalít napr. site collection, subsites, URL hierarchiu, veľkosť kapacity, šablóny, ainé overenia pre uskutočnenie analýzy.

- Overenie, povolení a vlastníctva dát a stránok.
- Overenie customizácie a komponentov a taktiež integrácie ďalšími aplikáciami.
- Identifikovanie funkcií, ktoré neexistujú v SharePoint Online a návrh ich náhrad.
- Overenie, dostupnosť a stabilitu internetového pripojenia. Do analýzy je potrebné zahrnúť aj branch office-y Obstarávateľa Rýchlosti internetového pripojenia na lokalitách Obstarávateľa budú poskytnuté v čase vykonávania analýzy.
- Kontrola firewall-ov pre pripojenia služby Microsoft.
- Iné úkony (resp. podľa *best practice* Zhotoviteľa), ktoré sú potrebné na úspešné vykonanie analýzy on-premisového SharePoint prostredia.

Analýza existujúceho Tenantu minimálne v rozsahu:

- Analýza existujúceho tenantu podľa *best practice* Zhotoviteľa pre potreby migrácie do novovytváraného tenantu

Identifikácia závislostí, rizík a integrácií v rámci migrácie minimálne v rozsahu:

- Identifikácia závislostí, rizík a integrácií v rámci migrácie z pohľadu dostupnosti dát Obstarávateľa v jeho systémoch
- Identifikácia závislostí, rizík a integrácií v rámci migrácie z pohľadu integrity a validácie.
- Iné úkony (resp. podľa *best practice* Zhotoviteľa), ktoré sú potrebné na úspešné vykonanie identifikácie závislostí, rizík a integrácií v rámci migrácie.

Analýza technických rizík a návrh minimalizácie rizika minimálne v rozsahu:

- Analýza rizika straty dát počas migrácie.
- Analýza rizika výpadku služieb.
- Kompatibilita užívateľských zariadení s navrhovanými službami a riešeniami v rozsahu tejto Zákazky
- Iné úkony (resp. podľa *best practice* Zhotoviteľa), ktoré sú potrebné na úspešné vykonanie analýzy technických rizík a návrhu minimalizácie rizika.

Analýza bezpečnostných rizík a návrh minimalizácie rizika minimálne v rozsahu:

- Riziká neautorizovaného prístupu akejkoľvek osoby alebo systému.
- Phishing, kybernetické útoky a iné hrozby majúce vplyv na činnosť Obstarávateľa.
- Iné úkony (resp. podľa *best practice* Zhotoviteľa), ktoré sú potrebné na úspešné vykonanie analýzy bezpečnostných rizík a návrhu minimalizácie rizika.

Analýza organizačných rizík a návrh minimalizácie rizika minimálne v rozsahu:

- Analýza nedostatkov školení a celkovej informovanosti používateľov.
- Analýza dostatočnosti zdrojov (napr. personálne kapacity) Obstarávateľa.
- Iné úkony (resp. podľa *best practice* Zhotoviteľa), ktoré sú potrebné na úspešné vykonanie analýzy organizačných rizík a návrhu minimalizácie rizika.

Identifikácia post-implementačných rizík a návrh minimalizácie rizika minimálne v rozsahu:

- Posúdenie a identifikácia príp. nezaznamenaných technických problémov.
- Posúdenie a identifikácia príp. nedostačujúcej hypercare.
- Posúdenie a identifikácia príp. neefektívnej správy licencií.
- iné úkony (resp. podľa *best practice* Zhotoviteľa), ktoré sú potrebné identifikáciu postmigračných rizík a návrh minimalizácie rizika.

2.2 Návrh budúceho stavu (TO-BE)

Návrh licenčného modelu s potrebným počtom typových licencií minimálne v rozsahu

Identifikácia potrieb licencovania minimálne v rozsahu
- Zistenie počtu aktívnych používateľov a ich pracovné potreby.
- Kategorizácia používateľov. Návrh rozdelenia používateľov podľa úrovne prístupu a potrebných služieb.
- Služby Microsoft 365. Návrh identifikácie služby, ktoré budú používatelia potrebovať (napr. Exchange Online, Teams, SharePoint, OneDrive).

Optimalizácia licencií minimálne v rozsahu
- Priradenie licencií na základe potrieb konkrétnych používateľov.
- Návrh nákupu licencií z pohľadu finančnej optimalizácie (finančne najvýhodnejšie riešenie pre zabezpečenie potrieb Obstarávateľa).
- Použitie analytických nástrojov. Návrh využitia napr. Microsoft 365 Admin Center, alebo podobný nástroj na sledovanie využitia licencií a odhalenie potenciálnych úspor.

Implementácia a správa licencií minimálne v rozsahu
- Nastavenie politik. Definovanie politiky na pravidelný audit licencií a ich optimalizáciu.
- Monitorovanie používania. Sledovanie pridelených licencie a ich využitie s vypracovaním správy 1x6 mesiacov.
- aktualizácia licenčných plánov na základe zmien v organizácii. 1x6 mesiacov

Návrh architektúry a technických komponentov minimálne v rozsahu

Návrh cieľovej architektúry pre implementované riešenia a služby minimálne v rozsahu:
- *High-level* (HL) popis cieľovej architektúry.
- *Low-level* Diagram (LLD) cieľovej architektúry.
- Podrobný dokument s presným popisom jednotlivých krokov a nadväzností počas a po migrácií.
- Návrh má obsahovať minimálne: cieľovú architektúru v Microsoft 365, Azure Active Directory a identitu, e-mailovú infraštruktúru, Sharepoint infraštruktúru, migráciu dokumentov a súborov, Microsoft Teams a kolaboračné služby, OneDrive, Intune a správu zariadení, zabezpečenie a compliance, licencovanie a náklady, technické komponenty migrácie, harmonogram a plán migrácie, požiadavky na HW/SW;

- a iné úkony (resp. podľa *best practice* Zhotoviteľa), ktoré sú potrebné pre prípravu návrhu/dokumentu o cieľovej architektúre.

Návrh kapacity siete a zálohovania minimálne v rozsahu

Návrh kapacity siete

- Internetová konektivita, šírka pásma, prípadne návrh QoS pre Teams, optimalizácia WAN pre pobočky.
- firewall prístupy, povolenia URL a IP rozsahov, SSL inšpekcia, IPD/IDS.
- DNS (MX, AUtodiscover, SPF, DKIM, DMARC)

Návrh zálohovania

- Ciele a požiadavky, RTO/RPO, retencia záloh, požiadavky na zabezpečenie plnenia povinností v zmysle právnych predpisov na úseku archívnictva a registratúry.
- Zálohované služby: Exchange Online, Sharepoint Online, OneDrive, Teams.

2.3 Príprava detailného časového plánu dodávky riešenia podľa tejto Technickej špecifikácie/riešení) spolu s definovanými míľnikmi

Definovanie fáz, kľúčových míľnikov, prechodových období minimálne v rozsahu

Návrh časového harmonogramu migrácie minimálne v rozsahu pre:

- Prípravná a analytická fáza s trvaním najviac 2 mesiace od nadobudnutia účinnosti zmluvy.
- Implementačná fáza s trvaním najviac 6 mesiacov od protokolárneho prevzatia prípravnej a analytickej fázy a dodania potrebných licencií špecifikovaných v návrhu TO-BE stavu. Implementáčná fáza sa môže po dohode Obstarávateľa a Zhotoviteľa predĺžiť na základe výstupov z “to be” analýzy v rámci prípravnej fázy, a to maximálne o 2 (slovom: dva) mesiace a za predpokladu súčasného naplnenia podmienok uvedených v bode 3.4. článku Zmluvy o dielo o poskytovaní služieb
- Post-implementačná fáza *Hypercare v trvaní* 3 mesiace od protokolárneho prevzatia implementačnej fázy.

- Školenia zamestnancov v priebehu implementačnej fázy podľa požiadaviek Obstarávateľa

- Produkčná fáza v trvaní do konca platnosti zmluvy od protokolárneho prevzatia post-implementačnej fázy.

Harmonogram musí obsahovať fázy minimálne v rozsahu v akom sú uvedené v prílohe“ Cenová ponuka”

2.4 Implementácia a systémové integrácie

Nasadenie Microsoft 365 služieb na základe Objednávateľom akceptovaných výstupov Prípravnej a analytickej fázy a návrhu TO-BE stavu minimálne v nasledujúcom rozsahu:

- Založenie nového Tenantu.
- Aktivovanie požadovaných služieb.
- Príprava on-premisového prostredia, vrátane Exchange SE pre hybridnú konfiguráciu.
- Aktualizácia on-premise AD na najnovšiu podporovanú verziu (ak bude súčasťou navrhovaného riešenia).
- Nová inštalácia Microsoft Entra Connectu na dedikované servery.
- Nastavenie hybridnej konfigurácie AD a Exchange.
- Nakonfigurovanie synchronizácie hesiel alebo pass-through autentifikácie Synchronizácie objektov podľa plánu a nastavenie Microsoft Entra Connect.
- Zabezpečenie správnosti UPN (User Principal Name) pre všetkých migrovaných používateľov.
- Migrácia identifikovaných kritických GPO.
- Aktivácia politík v Intune pre konfiguráciu zariadení, ktoré zodpovedajú on-premise GPO.
- Migrácia objektov, synchronizácia dotknutých používateľov, skupín a počítačov.
- Integrácie AD & SAP, GIS (Geograficky informačný systém), eHuman (HR system), CDesk (It ticketing system), Registratúra (Memphis), DMS systém, eGOV (eSlovensko)
- Iné postupy a úkony podľa *best practice* a výstupu analýzy TO-BE stavu.

Migrácia dát (pošta, dokumenty, SharePoint) minimálne v rozsahu:

- Migrácia dát z existujúceho Tenantu (Sharepoint, OneDrive, Teams) na základe výstupov “as is” analýzy existujúceho tenantu
- Vytvorenie dávok migrácie pre Exchange aj pre Sharepoint.
- Pre Exchange rozdelenie používateľov na dávky na základe analýzy a návrhu.
- Pre Sharepoint rozdelenie dát na základe analýzy a návrhu.
- Monitorovanie priebehu migrácie.
- Overenie migrácie. Kontroly po dokončení každej dávky, že či všetky dáta boli správne prenesené (e-maily, kalendáre, kontakty, dáta z Sharepoint-u.).
- Dokumentácia progresu migrácie s kontrolnými bodmi.

- Iné postupy a úkony podľa *best practice* Zhotoviteľa a výstupu návrhu TO-BE stavu.

Nastavenie zabezpečenia, compliance a governance - na základe analýzy a návrhu pripraveného Zhotoviteľom

- Tenant Security Hardeninig podľa návrhu.
- Information protection podľa návrhu.
  Zapnutie Outlook message encryption podľa návrhu.

- Microsoft Entra Privileged Identity Management.
- Implementácia Microsoft Defender for Endpoint ako náhrada pre antivírus tretích strán s EDR.
- Aktivácia Microsoft Defender pre identity.
- Aktivácia Microsoft Defender pre Office 365.
- Data loss prevention (AIP – klasifikácia dát) podľa návrhu.
- Nasadenie DLP podľa licencií a podľa návrhu (nie je súčasťou základnej implementácie a bude riešené individuálne na samostatnú objednávku Obstarávateľa).
- Aktivácia MFA, Conditional Access Policies.
- Nasadenie Microsoft Purview eDiscovery solutions.
- Implementácia Cloud Adoption Framework Enterprise Scale Landing zónu v súlade s klasifikáciou definovanou MIRRI v kategóriách U1-U3.
- Microsoft Entra Privileged Identity Management a vytvorenie matice prístupov pre privilegované účty.
- Stanovenie perimetra bezpečnosti Cloudových služieb ako sú Identita, Elektronická pošta, Správa koncových staníc, Microsoft Teams, Microsoft Sharepoint, Microsoft OneDrive, Power Platform, Bezpečnosť, Monitoring, Microsoft Azure,a to v súlade so štandardami aplikovateľnými pre cloudové služby a hybridnú infraštruktúru podľa CIS, ISO 27001, NIS2 a iných záväzných právnych predpisov na úseku kybernetickej bezpečnosti.) Vybudovanie centrálneho logovacieho riešenia na platforme Log analytics pre zabezpečenie retencie auditnej stopy na 12 mesiacov. Riešenie musí obsahovať celú auditnú stopu, ktorú budú generovať všetci zamestnanci BVS, externisti a využívané služby M365.

Zabezpečenie zálohovania

- Návrh stratégie zálohovania cloudových služieb - pre zálohy dát z Exchange online, Sharepoint online a OneDrive v rámci:
  - Microsoft zálohovanie v rámci M365 licencií, odhadovaná veľkosť zálohovania je 10TB v prvom roku;
  - „M365 Backup“ add-on alebo pomocou iného adekvátneho riešenia. Azure subskripcia (s prihliadnutím na výšku kreditu, ktorý zabezpečí Obstarávateľ)
  - Azure files – sync do lokálneho servera;

Súčasťou návrhu „TO-BE“ stavu bude aj návrh ukladania záloh aj mimo dátových centier Microsoft-u ale na území EU z dôvodu zabezpečenia GDPR

Hypercare – po dobu 3 mesiacov od čiastkového protokolárneho prevzatia diela Fáza č. 4a na Microsoft 365 minimálne v rozsahu:

- Zabezpečenie podporných tímov a komunikačnej matice napr. pre: IT administrátori, Support (1st & 2nd level), Špecialisti na M365 (Exchange Online, SharePoint, Intune, atď.), Projektový manažér / Koordinátor.
- Zabezpečenie kanálov podpory pre používateľov napr.: mail, telefón (hotline), Teams kanály, a podobne, na základe dohody s Obstarávateľom, dostupných Obstarávateľovi v režime 24/7.
  Zabezpečenie špecialistov najmä na /najčastejšie sa vyskytujúce problémy ako sú napr.: problémy s prihlásením do Microsoft 365, nezobrazené alebo chýbajúce e-maily po migrácii, nefunkčný Outlook, Teams, OneDrive, Sharepoint, nesprávna synchronizácia medzi zariadeniami, aktivácia Office balíka, licencií, atď.
- Zabezpečenie zvýšeného monitoringu synchronizácie, logov, bezpečnostných nálezov, atď.
- Sprístupnenie záznamov zo školení v prípade potreby Obstarávateľa.
- Na záver formálneho ukončenia Hypercare obdobia je potrebná aktualizácia dokumentácie, zohľadnenie spätnej väzby a nahlásených problémov od používateľov, spracovanie ankety a splnenie požadovanej úrovne implementácie a systémovej integrácie prostredníctvom dosiahnutia požadovaných KPIs.
- *Key Performance Indicator* (tzv. **KPI**; kľúčový ukazovateľ výkonnosti) vo vymedzenom rozsahu: počet incidentov, čas vyriešenia, % znovuotvorených tiketov Metrika hodnotenia KPIs:
  - **1. Počet incidentov**
    - Definícia: Celkový počet nahlásených incidentov počas Hypercare.
    - Cieľová hodnota pre ukončenie fázy "4b Hypercare" je *: 5/0 pre kritické incidenty, 15/0 pre závažné incidenty, 50/0 pre bežné incidenty

  * Zavedenie **dvojúrovňového modelu (X/Y)**, kde:
- **X** je maximálny počet incidentov, po ktorého prekročení sa považuje KPI za **nesplnené;**
- **Y** predstavuje počet incidentov, ktoré sú **nevyriešené**
- Segmentácia:
  - Podľa typu služby samostatne (Exchange Online, Teams, SharePoint, OneDrive…).
  - Podľa závažnosti (rozdelenie incidentov v zmysle delenia uvedeného v časti 2.7.1. nižšie na kritické, závažné, bežné)

  - **2. Priemerný čas vyriešenia incidentu (Time to Fix)**
    - Definícia: Priemerný čas od nahlásenia incidentu po jeho vyriešenie.
    - Upresenie, čo sa považuje za vyriešenie incidentu je uvedené c bode 8.7 Zmluvy o dielo o poskytovaní služieb
    - Cieľová hodnota:
      - **kritická**: reakčná doba (tzv. response time) do 1 hodiny, vyriešenie incidentu (tzv. time to fix) do 4 hodín
      - **závažná**: reakčná doba (tzv. response time) do 1 hodiny, vyriešenie incidentu (tzv. time to fix) do 1 pracovného dňa

- **bežná**: reakčná doba (tzv. response time) do 6 hodín, vyriešenie incidentu (tzv. time to fix) do 3 pracovných dní

- **3. Percento znovuotvorených incidentov**
  - Definícia: Percento incidentov zapríčinených Zhotoviteľom, ktoré boli uzavreté, ale neskôr znovu otvorené kvôli neadekvátnemu (nedostatočnému) vyriešeniu.
  - Vzorec:
    Reopen Rate = (Počet znovuotvorených incidentov / Celkový počet incidentov) × 100%R
  - Cieľová hodnota: < 5 %

Ak na záver formálneho ukončenia Hypercare obdobia (3 mesiace) nie sú splnené KPIs vo vymedzenom rozsahu, dôjde k predĺženiu Hypercare obdobia o jeden mesiac, v rámci ktorého Zhotoviteľ zabezpečí, aby boli prijaté primerané opatrenia identifikáciu možných príčin na zabezpečenie riadneho nasadenia služieb M365, t.j. aby v rámci implementácie a systémovej integrácie boli uskutočnené také opatrenia, ktoré zabezpečia úroveň požadovaného rozsahu KPIs.

Návrh, realizácia, vyhodnotenie Adopčnej kampane

Cieľom adopčnej kampane je zabezpečiť úspešné prijatie a aktívne využívanie nového softvérového riešenia koncovými používateľmi. Zhotoviteľ je povinný poskytnúť návrh adopčnej kampane a zabezpečiť realizáciu a podporu pri spustení a vedení adopčnej kampane a to už v rámci implementačnej fázy v súlade s metodikou Fast Track for Microsoft 365.

Požiadavky na metodiku a postup:

1. **Metodika nasadenia:** Zhotoviteľ je povinný realizovať všetky činnosti v súlade s metodikou FastTrack for Microsoft 365, ktorú definuje spoločnosť Microsoft ako oficiálny rámec pre plánovanie, nasadenie a adopciu cloudových služieb Microsoft 365.
2. **Fázy realizácie musia zahŕňať:**
   a. Envision (Návrh Zhotoviteľa): Stanoviť víziu, návrh KPIs na základe rámca definovaného v metodike FastTrack , vybrať scenáre a navrhnúť tím v spolupráci s Obstarávateľom (sponzor, *Success Owner, Champions, Early Adopters*).
      i. Identifikácia obchodných cieľov a scenárov využitia služieb Microsoft 365.
      ii. Vypracovanie plánu nasadenia a stratégie prijatia technológie.
   b. Onboard (Nasadenie): technicky pripraviť Tenant, pilotovať, spustiť komunikáciu a tréning.
      i. Technická príprava prostredia (identity, bezpečnosť, compliance). ii. Migrácia e-mailov, súborov a používateľských účtov
   c. Drive Value (Adopcia): škálovať na celú firmu, merať používanie a neustále podporovať adopciu.
      i. Podpora používateľov pri osvojovaní si nových nástrojov.
      ii. Poskytnutie tréningových materiálov, šablón a odporúčaní na zvýšenie produktivity.
3. **Výstupy a dokumentácia:**

- Zhotoviteľ predloží plán nasadenia, zoznam vykonaných aktivít podľa metodiky FastTrack a dokumentáciu k adopcii používateľov.
- Súčasťou výstupu bude aj návrh na ďalšie zlepšenie využívania Microsoft 365 služieb.

Overenie splnenia:

- Obstarávateľ si vyhradzuje právo požadovať dôkaz o dodržaní metodiky (napr. výstupy z FastTrack portálu, komunikácia s Microsoft tímom, štruktúra implementácie a adopcie).

2.5 Školenie zamestnancov

Súčasťou predmetu zákazky je aj realizácia školení v slovenskom alebo českom jazyku vrátane dodania vzdelávacích materiálov na aplikácie ako Word, Excel, PowerPoint, OneNote, Microsoft Teams a Microsoft Copilot, ako aj ďalšieho softvéru a nástrojov. Súčasťou každého školenia je aj vypracovanie vzdelávacích materiálov a prezentácie, ktoré budú odovzdané / zaslané účastníkom školenia. Pod pojmom "školiaci deň" Obstarávateľ požaduje školenie v celkovom trvaní 8 hodín.

2.5.1 Školenie pre IT administrátorov

Preferovaná forma školení je prezenčne prostredníctvom workshopov. Jedná sa o skupinu 10 ľudí. Požadovaná doba školení je 10 školiacich dni. Minimum požadovaného obsahu školení:

a. **Správa Microsoft 365 Tenant-u:**
   - Konfigurácia organizačného profilu.
   - Možnosti predplatného Tenant-u.
   - Správa používateľských účtov a licencií.
   - Bezpečnostné skupiny a administratívne role.

b. **Synchronizácia identít:**
   - Azure Active Directory Connect.
   - Connect Cloud Sync.
   - Správa synchronizovaných identít a jednotného prihlasovania (SSO). Multifaktorová autentifikácia a samoobslužná správa hesiel.

c. **Bezpečnosť a ochrana:**
   - Microsoft Secure Score.
   - Azure Active Directory Identity Protection.
   - Exchange Online Protection, Safe Attachments, Safe Links.
   - Microsoft 365 Defender, Microsoft Defender for Cloud Apps, Microsoft Defender for Endpoint.
   - Analýza logovania.

d. **Compliance a správa dát:**

- Archivovanie a uchovávanie dát.
- Šifrovanie správ Microsoft Purview.
- Prevencia straty dát (DLP).
- Insider risk management, informačné bariéry, DLP politiky.
- Klasifikácia dát a citlivé štítky.
- Analýza hlásení a reportovanie.

Súčasťou školenia sú aj školiace materiály - skriptá (v tlačenej podobe v slovenskom jazyku) a prezentácia, ktorá bude odovzdaná / zaslaná účastníkom elektronicky. Školiace materiály dostanú účastníci na mieste pred začiatkom školenia, prezentácia môže byť zaslaná elektronicky.

2.5.2 Školenia „Train the trainer“ pre super-users

Preferovaná forma školení je prezenčne prostredníctvom workshopov. Jedná sa o skupinu 30 ľudí. Požadovaná doba školení sú 4 školiace dni v 3 skupinách po 10 ľudí. Celkovo sa uskutoční 12 školiacich dní. Minimum požadovaného obsahu školení:

a. **Základy Microsoft 365:**
   - Prehľad služieb a aplikácií Microsoft 365.
   - Navigácia v prostredí Microsoft 365.
   - Základné funkcie a možnosti aplikácií ako Outlook, Teams, OneDrive, SharePoint, Copilot, Forms, Planner.

b. **Komunikácia a spolupráca**
   - Používanie Microsoft Teams na chatovanie, videohovory a spoluprácu.
   - Zdieľanie dokumentov a spolupráca na nich v OneDrive a SharePoint.
   - Správa e-mailov a kalendárov v Outlooku.

c. **Správa súborov**:
   - Ukladanie a organizácia súborov v OneDrive.
   - Zdieľanie súborov s kolegami a externými partnermi.
   - Spolupráca na dokumentoch v reálnom čase.

d. **Bezpečnosť a ochrana dát**:
   - Základy bezpečnosti v Microsoft 365.
   - Rozpoznávanie phishingových e-mailov a ochrana pred hrozbami.
   - Používanie citlivých štítkov na ochranu citlivých informácií.

e. **Efektívne využívanie aplikácií**:
   - Tipy a triky na zvýšenie produktivity v aplikáciách Microsoft 365.
   - Automatizácia úloh pomocou nástrojov ako Power Automate.
   - Využívanie integrácií medzi aplikáciami na zjednodušenie pracovných procesov.

f. **Analytika a reporty**:

- Využívanie analytickej funkcie hlásení a tvorba reportov.

Súčasťou školenia sú aj školiace materiály - skriptá (v tlačenej podobe v slovenskom jazyku) a prezentácia, ktorá bude odovzdaná / zaslaná účastníkom elektronicky. Školiace materiály dostanú účastníci na mieste pred začiatkom školenia, prezentácia môže byť zaslaná elektronicky.

2.5.3 Koncoví používatelia

Forma školenia: online webinár s minimálnou kapacitou 500 účastníkov.
Dĺžka trvania 1 webináru = 1 školiaci deň (8 hodin)
Webinár môže byť rozdelený na niekoľko individuálnych blokov v priebehu dní.

Zhotoviteľ uskutoční po dohode s Obstarávateľom 3 termíny tejto vzdelávacej aktivity pričom z každej vyhotoví audiovizuálny záznam, pričom tie Obstarávateľ následne bude používať pre svoje interné vzdelávacie účely (e-learningové moduly vo vlastnom e-learningovom systéme). Zhotoviteľ teda udelí Obstarávateľovi bezvýhradnú licenciu na použitie audiovizuálneho diela.

Pre každý tematický okruh školenia (napr. Základy Microsoft 365, Komunikácia a spolupráca atď.) Zhotoviteľ vytvorí aj súbor min. 25 testových otázok, ktoré poskytne Obstarávateľovi pre potreby testovania zamestnancov v rámci interného e-learningového systému. Súbor otázok mu zašle najneskôr do 5 pracovných dní po realizácií posledného termínu webináru.

Cieľovou skupinou webináru sú zamestnanci - bežní používatelia - v počte cca 1100. Minimum požadovaného obsahu školení. Potreba dodať základné a pokročilé školenia.

a. **Základy Microsoft 365:**
   - Prehľad služieb a aplikácií Microsoft 365.
   - Navigácia v prostredí Microsoft 365.
   - Základné funkcie aplikácií ako Outlook, Teams, OneDrive, SharePoint.

b. **Komunikácia a spolupráca**
   - Používanie Microsoft Teams na chatovanie, videohovory a spoluprácu.
   - Zdieľanie dokumentov a spolupráca na nich v OneDrive a SharePoint.
   - Správa e-mailov a kalendárov v Outlooku.

c. **Správa súborov**:
   - Ukladanie a organizácia súborov v OneDrive.
   - Zdieľanie súborov s kolegami a externými partnermi.
   - Spolupráca na dokumentoch v reálnom čase .

d. **Bezpečnosť a ochrana dát**:
   - Základy bezpečnosti v Microsoft 365.
   - Rozpoznávanie phishingových e-mailov a ochrana pred hrozbami.
   - Používanie citlivých štítkov na ochranu citlivých informácií.

e. **Efektívne využívanie aplikácií**:
   - Tipy a triky na zvýšenie produktivity v aplikáciách Microsoft 365.
   - Automatizácia úloh pomocou nástrojov ako Power Automate.
   - Využívanie integrácií medzi aplikáciami na zjednodušenie pracovných procesov.

Súčasťou webináru sú aj školiace materiály - skriptá (v elektronickej podobe v slovenskom jazyku) a prezentácia, ktorá bude odovzdaná účastníkom. Školiace materiály musia byť zaslané účastníkom minimálne 2 dni pred konaním webináru. Prezentácia im môže byť zaslaná po skončení webináru.

2.6 Dokumentácia

Obstarávateľ požaduje, aby boli priebežne dodávané nasledovné dokumenty minimálne v rozsahu:

2.6.1 Systémová, prevádzková dokumentácia má obsahovať minimálne:

- Podrobný technický popis novej infraštruktúry v M365 (Solution design).
- Architektúra služieb (Exchange Online, SharePoint Online, Teams, OneDrive, Azure AD atď.). Podrobný LLD diagram, vrátane z pohľadu infraštruktúry a z pohľadu aplikácií.
- Popis identity modelu (napr. hybridná identita, Azure AD Connect).

Zoznam použitých licenčných plánov a ich pridelenie používateľom.

- Zoznam konfigurácií zabezpečenia (MFA, Conditional Access, Defender for M365, DLP, MIP).
- Prehľad o správe zariadení (Intune, Autopilot, registrácia).
- Minimálne ročná aktualizácia systémovej dokumentácie (technickej, prevádzkovej) vždy ku dňu výročia účinnosti zmluvy počas celej doby jej trvania. Každá systémová zmena musí byť dopracovaná do systémovej dokumentácie.
- Raz ročne dopracovaný security assesment a health check.

2.6.2 Disaster Recovery Plan (DRP) má obsahovať minimálne:

- Scenáre obnovy jednotlivých služieb (napr. obnovy mailboxov, dokumentov, tímov). • Obnova konfigurácií Tenatu (napr. skupinové politiky v Intune, nastavenia Defenderu).
- Zodpovednosti a kontakty pri DR situáciách.
- Definovanie časových rámcov RTO/RPO podľa jednotlivých služieb.
- Popis použitia nástrojov tretích strán pre zálohovanie.
- Step-by-step popis obnovy.
- Ročný backup-restore test so spracovaním harmonogramu činností.

2.6.3 Kvartálna správa o profylaxii má obsahovať minimálne:

- Vyhodnotenie systémovej dostupnosti a výpadkov.
- Odporúčania na vylepšenie výkonu a stability služieb.
- Prehľad preventívnych opatrení za predchádzajúci mesiac.
- Report o aktualizáciách konfigurácií a licencovania.

2.6.4 Mesačná bezpečnostná správa má obsahovať minimálne:

- Záznamy o bezpečnostných incidentoch a ich riešení.
- Prehľad aktivít týkajúcich sa zabezpečenia (napr. detekcie pokusov o prístup).
- Prehľad auditov a logovania (napr. sign-in logs, audit logs).
- Change management nastavených politik
- Odporučenia a návrhy na zlepšenie bezpečnosti.
- Mesačná bezpečnostná správa je podklad na mesačnú fakturáciu.
- Záznamy o patchovaní.
- Záznamy o zmene admin prístupov.
- Záznamy o zmene bezpečnostného skóre, vyhodnotene na mesačnej báze.

2.6.5 Matica prístupov do M365 Tenantu má obsahovať minimálne:

- Zoznam interných a externých rolí s definovanými právami.
- Rozdelenie podľa správy: Global Admin, Exchange Admin, Security Reader, Compliance Admin
- Odporúčania na princíp minimálnych práv (Least Privilege).
- Identifikácia privilegovaných účtov a odporúčané zabezpečenie.
- Change management prístupov

2.6.6 Komunikačná matica má obsahovať minimálne:

- Definícia komunikačných liniek počas projektu migrácie a aj počas produkcie
- Kontaktné osoby z radov Obstarávateľa, Zhotoviteľa, tretích strán.
- Zodpovednosti a eskalačné kontakty.
- Spôsob oznamovania zmien, výpadkov a incidentov.

2.6.7 Návrhy smerníc pre Obstarávateľa týkajúcich sa predmetu implementácie podľa tejto Technickej špecifikácie má obsahovať minimálne:

Obstarávateľ požaduje vypracovanie návrhov (tzv. „*draft*“) interných smerníc Obstarávateľa v slovenskom jazyku.
Obstarávateľ požaduje, aby boli priebežne (po dohode Obstarávateľa a Zhotoviteľa) dodávané dokumenty v minimálne nasledujúcom obsahu informácií:

- jednoznačný popis aktivít a činností, ktoré majú byť vykonané,
- termíny a lehoty, v ktorých majú byť aktivity a činnosti vykonané,
- spôsob dokumentácie výkonu procesných aktivít a činností,
- spôsob kontroly výkonu procesných aktivít a činností,
- procesné role pri výkone aktivít a činností a nositeľov zodpovednosti,
- vstupy a výstupy procesných aktivít a činností,
- súlad s platnými právnymi predpismi
- optimálne a efektívne využitie zdrojov spoločnosti,
- riziká procesu.

Minimálny rozsah návrhov smerníc musí obsahovať:

a) Prevádzková smernica

- Zodpovedné osoby (IT oddelenie / externý správca)
- Definovanie procesov prevádzky M365 služieb. Pravidlá pre pridelenie licencií.
- Definovanie pravidiel pre správu účtov, distribučných skupín, záloh a obnovy.
- Definovanie Incident Manažmentu, povinnosti a časové lehoty (SLA).
- Definovanie zmenových konaní, schvaľovateľov, testovanie a dopady.

b) Používateľská smernica

- Pravidlá pre používanie služieb (napr. Teams, Outlook, SharePoint).
- Pravidlá na ukladanie súborov a pravidlá ich zdieľania.
- Pokyny k zodpovednému používaniu (phishing, zdieľanie dát).
- Postupy v prípade straty zariadenia či kompromitácie účtu.
- Základná kybernetická bezpečnosť, ako napríklad zapnúť MFA, okamžite hlásiť incident na odbor bezpečnosti.
- Odpovede na časté otázky (FAQ), napr.: Ako si obnoviť heslo?, Čo robiť pri zaplnení úložiska?, a pod.

c) Bezpečnostná smernica

- Definuje pravidlá MFA, správy hesiel, zdieľania, ukladania a prístupu k dátam. • Zadefinovanie princípov minimálnych práv (Least Privilege Access)
- Politiky šifrovania, Data Loss Prevention, prístupu z externých sietí.
- Zadefinovanie pravidiel monitorovania, zapnutú úroveň logovania a prístupy k logom.
- Definovanie Incident Manažmentu, povinnosti a časové lehoty (SLA).
- Postupy pri kompromitovaní účtu.
- Definovanie zmenových konaní, schvaľovatelia, testovanie a dopady.
- Definovanie revízie, kontrol, interných auditov privilegovaných účtov.

2.7 Technická podpora

Predmetom zákazky je zabezpečenie technickej podpory, rozvoja a bezpečnosti cloudových Microsoft platforiem a riešení založených na technológiách M365 a Microsoft Azure prevádzkovaných BVS.

Požiadavka Obstarávateľa je zabezpečenie technickej podpory zo strany Zhotoviteľa v slovenskom alebo českom jazyku.

Celková dĺžka poskytovania služieb technologickej podpory a rozvoja je 24 mesiacov od termínu dodania služieb špecifikovaných v v prílohe “Cenová ponuka”, špecificky po ukončení fázy “4b - Hypercare”.

2.7.1 Štandardná reaktívna podpora

Technická telefonická podpora, emailová podpora, podpora prostredníctvom tiketovacieho portálu (dostupný 24/7), konzultácie, asistencia online alebo na mieste v prípade potreby a/alebo nemožnosti vykonať podporu on-line v režime 8 x 7, v čase od 8:00 do 16:00 a to v rozsahu služieb a pravidelné úkony podpory:

- Správa incidentov a ich problémov v prípade zlyhania lokálnej alebo cloudovej technológie spoločnosti Microsoft.
- Návrh riešenia zistených problémov, realizácia zmien a požiadaviek v nastaveniach zistených z monitoringu.
- Dohľad nad prevádzkou a kontrola zálohovania.
  (*vyššie uvedené činnosti podpory sú vykonávané priebežne, podpora je poskytovaná čo najskôr po jej nahlásení*)

- Validácia a aktualizácia testovacieho prostredia voči produkčnému prostrediu (postačuje realizovať max. 4 x ročne).
- Ročný „*backup-restore*“ test so spracovaním harmonogramu činností (na mieste). Koordináciu s dodávateľmi aplikácií zabezpečí Obstarávateľ. Výstupom má byť podrobná auditná správa o úspešnosti. Za splnenie sa považuje úspešne ukončená obnova systémov. V prípade neúspechu sa testy opakujú. Koordináciu s dodávateľmi aplikácií zabezpečí Obstarávateľ. Plánované „*disaster restore*“ testy Obstarávateľ nahlási najneskôr 10 pracovných dní pred uskutočnením.
- Ročná aktualizácia systémovej dokumentácie (technickej, prevádzkovej) k výročiu zmluvy počas celej doby jej trvania.

Incident manažment:

Prevádzkové hodiny služby : 7 dní v týždni, 8 hodín denne od 08:00 do 16:00

Reakčná doba sa uplatňuje iba v rámci prevádzkových hodín služby.

Za reakčnú dobu sa považuje doba od nahlásenia vady incidentu Zhotoviteľovi stanoveným spôsobom, do spätného potvrdenia nahláseného incidentu Objednávateľovi. Zhotoviteľ je povinný bezodkladne spätne potvrdiť nahlásenie incidentu oprávnenej osobe Objednávateľa. Spätné potvrdenie má deklaratórnu povahu pre začiatok plynutia doby riešenia. O čas reakčnej doby sa nepredlžuje doba vyriešenia incidentu, ktorá začína plynúť nahlásením incidentu Zhotoviteľovi stanoveným spôsobom.

Za dobu vyriešenia incidentu sa považuje doba od nahlásenia incidentu Zhotoviteľovi stanoveným spôsobom, do jej písomne odsúhlaseného odstránenia (tzv. *time to fix*).

Upresenie, čo sa považuje za vyriešenie incidentu je uvedené v bode 8.7 Zmluvy o dielo o poskytovaní služieb.

Pri klasifikácii incidentu (problému/vady) pre úroveň:

- **kritická:** reakčná doba (tzv. *response time*) do 1 hodiny, vyriešenie incidentu (tzv. *time to fix* do 4 hodín
- **závažná:** reakčná doba (tzv. *response time*) do 1 hodiny, vyriešenie incidentu (tzv. *time to fix*) do 1 pracovného dňa
- **bežná:** reakčná doba (tzv. *response time*) do 6 hodín, vyriešenie incidentu (tzv. *time to fix*) do 3 pracovných dní

Klasifikáciu incidentu:

- **Kritický incident** – kritická porucha, ktorá sa prejavuje výpadkom fungovania celého prostredia alebo jeho podstatnej časti a tak bráni alebo vážne ohrozuje použitie celého informačného systému (informačných systémov; vrátane M365) Obstarávateľa alebo takej jeho časti, ktorá zaisťuje hlavné procesy, alebo má vážny dopad na kvalitu dát, ak problém nemôže byť riešený zmenou postupu práce s Informačným systémom, t.j. neexistuje iné riešenie daného problému. Riešenie má najvyššiu prioritu.
- **Závažný incident** – vážna porucha, ktorá sa prejavuje výpadkom fungovania modulov a funkcií a tak závažným spôsobom obmedzuje funkčnosť informačného systému (informačných systémov; vrátane M365) Obstarávateľa alebo kvalitu dát, avšak neobmedzuje použitie prostredia ako celku alebo jeho podstatnej časti. Riešenie má vysokú prioritu
- **Bežný incident –** vada, ktorá nemá vplyv na hlavnú funkcionalitu informačného systému (informačných systémov; vrátane M365) Obstarávateľa. Riešenie má nízku prioritu.

Objednávateľ pri nahlasovaní incidentu uvedie jeho klasifikáciu.

Kvalita dostupnosti systému / služieb balíka M365 v zodpovednosti Zhotoviteľa:

Je požadovaná 99,90 % funkčnosť systému z celkového času prevádzky systému v jeho produktívnom prostredí každého kalendárneho mesiaca.

Výpočet dostupnosti systému:
Dostupnosť systému (ďalej lej „DS“) je vyjadrená v % a vypočíta sa podľa vzorca:

$$DS = \frac{(T_S - T_N)}{(T_S)} \times 100$$

Pričom
TS je dohodnutý čas prevádzky služby v mesiaci v minútach.

TN je súčet všetkých výpadkov služby v mesiaci v minútach, kde do TN sa nezapočítava:

a. doba ohlásených plánovaných odstávok;

b. doba ohlásených neplánovaných odstávok;

c. doba dočasného prerušenia poskytovania služby na žiadosť Obstarávateľa;
d. doba dočasného prerušenia poskytovania služby z dôvodu zmeny prevádzkových parametrov okruhu resp. služby na žiadosť Obstarávateľa (zmena rýchlosti a pod.), z dôvodu prekládky jedného koncového bodu na žiadosť Obstarávateľa a pod.;
e. doba prerušenia spôsobená Obstarávateľom alebo dôvodom na strane Obstarávateľa je najmä, ale nie len:
    - prerušenie spôsobené nevhodným používaním zariadení Zhotoviteľa zo strany Obstarávateľa alebo ich odpojením;
    - prerušenie spôsobené výpadkom elektrického napájania na strane

    Obstarávateľa;
f. doba počas, ktorej nebol umožnený prístup technickým pracovníkom Zhotoviteľa do priestorov, v ktorých je umiestnená infraštruktúra alebo koncový bod Obstarávateľa;
g. doba neposkytnutia súčinnosti zo strany Obstarávateľa pri poruche;
    - doba prerušenia zapríčinená nefunkčnosťou (aj opakujúcou sa) koncovýchzariadení, ktoré sú majetkom Obstarávateľa;

i. doba prerušenia z dôvodu nepredvídateľných a neodvrátiteľných udalostí (vyššia moc).

Meranie dostupnosti systému / služieb balíka M365 v zodpovednosti Zhotoviteľa:
Pravidelné vykonávanie merania a vyhodnocovania dostupnosti systému za každý kalendárny mesiac na základe výstupov systému pre evidenciu, správu a riešenie nahlásených porúch (Service desk). Obstarávateľ má taktiež právo na meranie dostupnosti služby. V prípade nezhody vo výsledkoch merania bude môcť byť vykonané porovnanie nameraných hodnôt, prešetrenie všetkých zaznamenaných hodnôt.

2.7.2 Proaktívna podpora

Proaktívna podpora zahŕňa nasledovné činnosti, ktoré nespadajú do štandardnej reaktívnej podpory, a to mesačne v rozsahu 8 (slovom: osem) Osobohodín. Proaktívna podpora začne plynúť od ukončenia fázy 4b Hypercare definovanej v prílohe “Cenová ponuka”. Proaktívna podpora bude poskytovanáminimálne nasledovnom rozsahu:

Správa Microsoft cloud produktov: AD Connect, Hybridné AD, Azure AD, M365 E1-E5, EMS E3, Win E3, Microsoft PurView, PIM, Identity protection, Conditional access, Microsoft Endpoint Management (Intune, co management, Autopilot, Defender for office, Defender for cloud apps, EDR, MDM, MAM, Double Key Encryption, Key Vault, Microsoft Azure, Log Analytics, Azure Landing zóna, Azure Iaas, Azure PaaS, Azure SaaS,

Pravidelná profylaxia Microsoft cloud prostredia
Pravidelná profylaxia cloudových prostredí Microsoft zahŕňa súbor opatrení na minimalizáciu bezpečnostných rizík, zlepšenie výkonu a udržanie služieb v prevádzke v nasledovných oblastiach: Riadenie aktualizácie softvéru, Monitorovanie stavu služieb, Správa prístupových práv, Správa identít, Správa konfigurácie Zmluva o poskytovaní služieb – podpora prevádzky,

rozvoja a bezpečnosti Microsoft cloudových platforiem. Táto bude vykonávaná minimálne 1 krát za kvartál

Monitoring – Service Health a Log Analytics - požiadavka Obstarávateľa na poskytnutie sumárnych reportov v oblastiach:

Monitoring - Service Health pre M365 obsahuje informácie o stave služieb v rámci Microsoft 365 (M365), vrátane Exchange Online, SharePoint Online, OneDrive for Business, Microsoft Teams a ďalších. Tento nástroj poskytuje informácie o stavoch služieb, prehľady, zmeny stavov, upozornenia na problémy, plánované údržby a ďalšie informácie o výkonu služieb. Monitoring - Service Health pre M365 je veľmi užitočný pre IT administrátorov a používateľov M365, ktorí chcú sledovať a riešiť problémy so službami M365.

Log analytics je služba v rámci služby M365, ktorá zhromažďuje, ukladá a analyzuje údaje z rôznych zdrojov vrátane protokolov z aplikácií a systémov. Tento nástroj umožňuje správcom systému M365 zhromažďovať a analyzovať veľké množstvo údajov a poskytuje im prehľad o stave a výkonnosti rôznych komponentov a služieb v rámci systému M365.

Funkcia Log Analytics v systéme M365 umožňuje správcom zhromažďovať a analyzovať údaje z mnohých rôznych zdrojov, ako sú napríklad protokoly aplikácií a služieb, bezpečnostné udalosti, informácie o údržbe a aktualizáciách a mnohé ďalšie. Údaje sú uložené v centrálnom úložisku a správcovia môžu pomocou dotazov a vizualizácií analyzovať údaje a získavať z nich užitočné informácie.

Pomocou nástroja Log Analytics bude poskytovaný:

- monitoring výkonu a dostupnosti služieb a aplikácií v rámci systému M365;
- monitoring činnosti používateľov a zisťovanie anomálie a bezpečnostné hrozby;
- analýza zdrojov problémov a výpadkov;
- plánovanie údržby a aktualizácií s cieľom zlepšiť výkon a dostupnosť služieb; • získavanie užitočných informácií na plánovanie kapacity a rozvoj systému M365.

Message center – governance a sledovanie zmien
Podpora pri interpretácii, prioritizácií, kategorizácii, implementácii a komunikácii zmien oznamovaných prostredníctvom Message Center, prípadne iných, relevantných kanálov.

Štvrťročný workshop na nové funkcionality
Workshopy a private preview nových funkcionalít pre vyhodnotenie a plánovanie ich nasadenia podľa poskytnutých informácii Microsoftom.

Ročný security assesment a health check
Vypracovanie ročného security hodnotenia Microsoft cloud služieb prostredníctvom 7 kľúčových oblastí:

1. **Analýza rizík** - preskúmanie rizík (hrozieb, pravdepodobnosti a dopadu) pre informácie a/alebo systémy s cieľom minimalizovať riziko na prijateľnú úroveň.

2. **Riadenie súladu** - Proces zabezpečovania plnenia cieľov súladu (regulačných, politických alebo iných).

3. **Riadenie zraniteľností** - Proces riadenia zraniteľností systému s cieľom znížiť vystavenie hrozbám.

4. **Audit** - Proces preskúmania kontrol spolu s podpornými dôkazmi s cieľom zabezpečiť dodržiavanie politík a postupov.

5. **Riadenie udalostí a incidentov** - Proces riadenia potenciálnych a skutočných incidentov informačnej bezpečnosti a udalostí, ktoré poskytujú prehľad o takýchto incidentoch.

6. **Bezpečnostná kultúra** - Celkový postoj organizácie, pokiaľ ide o ľudí a procesy, súvisiace s bezpečnosťou informácií a systémov.

7. **Riadenie politík a procesov** - Proces riadenia, ktorý zabezpečuje formalizáciu, dokumentáciu, presadzovanie a revíziu aplikovaných politík a procesov.

Udržiavania technickej dokumentácie
Priebežná aktualizácia Solution design dokumentácie.

Revízia a aktualizácia Azure Landing zone
Implementácia nových funkcionalít a prípadných zmenených alebo nových požiadaviek regulácie a bezpečnosti.

Starostlivosť a aktualizácia testovacieho prostredia pre Microsoft cloud prostredie
Testovacie prostredie je použité pre pilotovanie nových funkcionalít a zmien v nastaveniach pred ich implementáciou v produkčnom prostredí.

Nevyčerpané osobohodiny sa prenášajú do nasledujúcich mesiacov v rámci toho istého kalendárneho roka.

Čerpanie je podmienené vystavením a odsúhlasením požiadavky zo strany Obstarávateľa.

2.7.3 Nadštandardná podpora

Podpora:

- vyžiadaná na základe písomnej požiadavky zaslanej Obstarávateľom, ktorá obsahuje opis požadovanej podpory, ktorá nespadá pod inú podporu (služby) poskytovanú (poskytované) v tejto zákazke;
- následne na základe požiadavky Zhotoviteľ uvedie časový návrh na vybavenie požiadavky ako aj opis plánovaných služieb, ktoré bude potrebné pre účely vybavenia požiadavky poskytnúť spolu s opisom príp. účinkov na rozsah služieb poskytovaných podľa tejto zákazky;
- Obstarávateľ v prípade súhlasu potvrdí formou objednávky realizáciu požiadavky alebo požiada o nové informácie v prípade úpravy pôvodnej požiadavky;
- Zhotoviteľ zabezpečí, aby vykonanie požiadavky bolo realizované takým spôsobom, ktorý je kompatibilný s poskytovaním plnenia podľa časti tejto zákazky.

Poskytovanie služieb v rámci nadštandardnej podpory v predpokladanom rozsahu maximálne 1600 Osobohodín počas celej doby 24 mesiacov plynúcej od ukončenia Fázy “4b Hypercare” definovanej v prílohe “Cenová ponuka”, pričom rozsah nie je Obstarávateľ povinný vyčerpať.

Všetky vykonané požiadavky musia byť zdokumentované a pridané do systémovej dokumentácie, pričom splnenie požiadavky sa odovzdáva prostredníctvom akceptačného protokolu.

Medzi požiadavky riešené v rámci nadštandardnej podpory môžu byť zahrnuté:

- Konzultácie v oblasti produktov Microsoft nad rozsah vymedzený v iných činnostiach v rámci tejto zákazky.
- Konzultácie v oblasti licenčnej politiky spoločnosti Microsoft nad rozsah vymedzený v iných činnostiach v rámci tejto zákazky.
- Konzultácie v oblasti Software Asset Management nad rozsah vymedzený v iných činnostiach v rámci tejto zákazky.
- Školenia používateľov v oblasti SW produktov Microsoft nad rozsah vymedzený v iných činnostiach v rámci tejto zákazky.
- Analytické a implementačné práce k produktom Microsoft Windows a Windows Server nad rozsah vymedzený v iných činnostiach v rámci tejto zákazky.
- Analytické a implementačné práce k produktom Microsoft DLP a XDR
- Analytické a implementačné práce k produktom Office 365 nad rozsah vymedzený v iných činnostiach v rámci tejto zákazky.
- Analytické a implementačné práce k produktom Enterprise Mobility & Security nad rozsah vymedzený v iných činnostiach v rámci tejto zákazky.
- Analytické a implementačné práce k produktom Microsoft Threat Protection nad rozsah vymedzený v iných činnostiach v rámci tejto zákazky.
- Analytické a implementačné práce k produktom Microsoft Information Protection & Governance nad rozsah vymedzený v iných činnostiach v rámci tejto zákazky.
- Analytické a implementačné práce k produktom Microsoft Azure nad rozsah vymedzený v iných činnostiach v rámci tejto zákazky.
- Analytické a implementačné práce k produktom Microsoft Power Platform nad rozsah vymedzený v iných činnostiach v rámci tejto zákazky.

- Analytické a implementačné práce k produktom Microsoft Power BI a Microsoft Fabric nad rozsah vymedzený v iných činnostiach v rámci tejto zákazky.
- Analytické a implementačné práce k produktom Microsoft Dynamics 365 nad rozsah vymedzený v iných činnostiach v rámci tejto zákazky.
- Analytické a implementačné práce v oblasti súladu so zákonom o kybernetickej bezpečnosti 69/2018 Z.z. a vyhlášky 362/2018 Z.z. nad rozsah vymedzený v iných činnostiach v rámci tejto zákazky.

Zoznam použitých skratiek

Skratka	Názov
AD	Active Directory
AIP	Azure Information Protection
API	Application Programming Interface
cDesk	portál na zadavenie tiketov
CIS	Center for Internet Security
CSP	Cloud Solution Provider
DAG	Directed Acyclic Graph
DKIM	DomainKeys Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DNS	Domain Name System
DR	Disaster Recovery
DRP	Disaster Recovery Plan
EDR	Endpoint Detection and Response
EMS	Enterprise Mobility + Security
FAQ	Frequently Asked Questions
GDPR	General Data Protection Regulation
GIS	Geograficko-informačný systém
GPO	Group Policy Object
HL	Hardware Layer
HW/SW	Hardvér/Softvér
IAM	Identity and Access Management
IDS	Intrusion Detection System
iOS	mobilný operačný systém vyvinutý spoločnosťou Apple
IP	Internet Protocol
IPD	Invasive Pneumococcal Disease
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
KPI	Key Performance Indicator
LLD	Low-Level Design
LTSC	Long-Term Servicing Channel

MAM	Mobile Application Management
MDM	Mobile Device Management
MFA	Multifactorová autentifikácia
MIP	Microsoft Information Protection
MIRRI	Ministerstva investícií, regionálneho rozvoja a informatizácie SR
MPSA	Microsoft Products and Services Agreement
MS	Microsoft
MSDN	Microsoft Developer Network
MX	Multiplexing
N/A	Not Applicable
NB	Notebook
NIS2	smernicu o bezpečnosti sietí a informačných systémov
NTLMv2	NT LAN Manager
Oauth	Open Authorization
Onprem	lokálne nasadené IT systémy
OoS	Online Operating System
OS	Operačný systém
PC	Počítač
PIM	Product Information Management
RBAC	Role-Based Access Control
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAP	Systems, Applications, and Products
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SPF	Sender Policy Framework
SSL	Secure Sockets Layer
SSO	Single Sign-On
TENANT	Logicky oddelené prostredie v rámci zdieľanej infraštruktúry
TLS	Transport Layer Security
U1- U3	Klasifikáciu úrovní kybernetických incidentov
UPN	User Principal Name
URL	Uniform Resource Locator
VoIP	Voice over Internet Protocol
WAF	Web Application Firewall
WAN	Wide Area Network