Příloha č. 2

Plán převzetí služeb a harmonogram

1. Plán převzetí služeb

KL01 – Obecné pravidelné služby a SLA

Popis návrhu převzetí služeb

Před převzetím služby je nutné nejdříve stanovit jasný plán převzetí. Tento plán musí obsahovat: Vymezení hlavních kontaktních osob, definice procesů, způsob omezování rizik, definice akceptačních kritérií a harmonogram převzetí služeb.

Pro převzetí uvedené služby je nutné analyzovat současný stav jednotlivých služeb a nastavených procesů. Následně bude nutné jasně specifikovat procesy v rámci převzetí služeb, a to zejména v oblasti kontroly změn, kontroly sporných skutečností a kontroly rizik v převzetí služby. Dále bude nutné vytvořit komunikační matici pro nastavení komunikačních kanálů v této oblasti pro zajištění informovanosti při přebíracím období. V rámci přebíracího období bude definován popis Implementačních kritérií, procesu testování a akceptace připravenosti na započetí poskytování cílových služeb. Při převzetí služeb budou zohledněny dopady na zaměstnance zadavatele, dopad na interní procesy a postupy koncového uživatele, připravenost vybavení, rozhraní a procesů nutných pro bezproblémové zahájení poskytování cílových služeb, finanční a obchodní dopady zahájení poskytování cílových služeb.

Převzetí této služby bude spojené s postupným převzetím dalších katalogových listů poskytovaných v rámci uvedené zakázky tak, aby bylo zajištěno plnění těchto obecně pravidelných služeb a celkového SLA.

Při přebíracím období je nutné stanovit harmonogram spuštění jednotlivých katalogových listů, aby bylo možné včasné zajištění plnění SLA parametrů pro jednotlivé služby.

Při převzetí této služby bude definována vzorová šablona pravidelného reportingu poskytovaných služeb, která bude obsahovat informace i poskytovaných službách a plnění těchto služeb dle nastavených hodnot SLA pro jednotlivé katalogové listy, které budou poskytovány. V přebíracím období musí být také nastaveny veškeré procesy spojené s poskytováním služeb jako je celkové nastavení služeb, testování provozu služeb, způsoby akceptace jednotlivých dílčích úkonů, řízení změnových požadavků a v neposlední řadě měření jednotlivých služeb. Dále bude nastavena kontaktní matice pro jednotlivé služby tak, aby bylo možné zajistit včasné informování o stavu poskytování uvedených služeb.

Před zahájením spuštění uvedení služby, bude prezentován stav převzetí služeb, navrhnutých procesů a doporučení pro zadavatele.

Před samotným zahájením plněním služby musí proběhnout akceptace této části, kde budou uvedeny veškeré detaily z průběhu analýzy a potvrzeny navrhnuté procesy.

Po této akceptaci dojde k plnohodnotnému poskytování uvedené služby a zahájeno reportování a plní SLA parametrů.

Přístup k řešení dané oblasti

Převzetí uvedené služby bude stanoveno dle standardních využívaných metodik a v závislosti na poskytovaných službách tak, aby nedošlo k omezení poskytovaných služeb a zároveň aby služba byla převzata s veškerými důležitými závislostmi na další poskytované služby a aby nedošlo k omezení těchto služeb během přebíracího období.

Tato oblast je nedílnou součástí všech dalších poskytovaných katalogových listů uvedených v zadávací dokumentaci a využívá vstupů pro reporting poskytovaných služeb. Tato služba zastřešuje ostatní poskytované katalogové listy z pohledu celkového plnění ICT služeb.

V rámci přebíracího období musí být jasně specifikovány měřitelné parametry dle jednotlivých katalogových listů, pro zajištění vyhodnocování těchto služeb. Pro zajištění měření těchto hodnot bude využita aplikace Helpdesk, kde jsou evidovány potřebné hodnoty dle uvedeného katalogového listu a také dohledový systém, který eviduje veškeré potřebné SLA parametry monitorovaných systémů. Tyto měřitelné hodnoty bude obsahovat pravidelný report, který bude uvádět seznam jednotlivých služeb a k nim naměřené hodnoty a tím i informace o stavu plnění jednotlivých služeb.

Metodický a procesní postup převzetí služeb

Pro zajištění převzetí uvedené služby bude použita projektová metodika PRINCE2® dle které budou zajištěny veškeré náležitosti, jako jsou:

- Celkové naplánování převzetí služby – seznam dílčích kroků, jejich vzájemných vazeb a termínů zahájení a ukončení
- Definice rizik v převzetí služby
- Koordinace třetích stran a optimalizace potřebné součinnosti při převzetí služby

Převzetí služby bude probíhat dle metodiky ITIL, která zajistí převzetí požadovaných služeb dle definovaných standardů. Použitá metodika bude řešit zejména níže uvedené oblasti.

- Definice požadované služby
- Nastavení služby
- Testovací provoz služby
- Validace služby
- Řízení změn
- Měření služby

Při převzetí služeb je nutné zohlednění metodik a politik v prostředí Zadavatele, a to zejména vydaných metodických pokynů a jednotlivých provozních řádů. Konkrétně se jedná o:

- Politika bezpečnosti informací Magistrátu hl. m. Prahy
- Technická bezpečnostní politika správy ICT
- Technická bezpečnostní politika sítí
- Technická bezpečnostní politika konfigurace ICT
- Instrukce pro přístup do oblastí zajištěných PZTS
- Metodický pokyn č. 7/2017–k řízení bezpečnostních událostí a bezpečnostních incidentů

- Metodický pokyn č. 8/2017 - Pravidla užívání informačního systému Magistrátu hl. m. Prahy
- Metodický pokyn č. 2/2018–k systému řízení IT služeb
- Metodický pokyn č. 1/2019 – Provozní řád datového centra DC4
- Metodický pokyn č. 2/2019 – Provozní řád datového centra DC5

Návrh harmonogramu

Detail činnosti	T+2	T+8	T+14	T+18	T+20
Příprava plánu převzetí					
Převzetí a seznámení se s dokumentací					
Provedení analýzy prostředí					
Převzetí seznamu spravovaného HW a SW					
Ověření platnosti kontaktní matice					
Ověření platnosti dodaných procesů					
Stanovení kontaktní matice pro jednotlivé systémy					
Příprava reportu SLA služeb					
Převzetí služby					

(T=počty dnů)

Požadovaná součinnost zadavatele

- Dodání seznamu a obsahu procesů pro dodávané služby
- Dodání dokumentace k provozovaným systémům
- Stanovení vzoru pravidelného reportingu
- Zajištění kontaktní matice provozovaných aplikací a systémů
- Dodání kompletního seznamu HW a SW
- Součinnost na přípravě pravidelného reportu služeb
- Předpokládaná součinnost zadavatele nepřesáhne 2 MD

Analýza rizik v dané oblasti

V rámci analýzy a řízení rizik je potřeba postupovat následujícími kroky „Identifikace" -> „Hodnocení" -> „Implementace". Analýza rizik je prováděna dle odhadnuté pravděpodobnosti a dopadu.

Pro převzetí uvedené služby jsme identifikovaly následující rizika:

Riziko	Hodnocení rizika	Návrh nápravného opatření
Nedodržení časového harmonogramu	Střední	Včasné zajištění veškerých potřebných podkladů a součinností pro převzetí služby
Nedostatečný přístup k informacím pro provedení analýzy	Střední	Včasné předání veškerých potřebných informací a přístupů pro provedení analýzy, správné nastavení

		komunikační matice
Nedostatečná nebo žádná dokumentace k systémům	Střední	Zajistit podporu objednatele, stanovení odpovědnosti na straně objednatele a zajištění potřebných vstupů. Detailní validace dokumentace vůči skutečnosti.
Poškození dat	Střední	Pro minimalizování rizika je nutné mít zajištěny zálohy dohledového systému
Nesoučinnost třetích stran	Střední	Včasné kontaktování třetích stran pro zajištění potřebných součinností, stanovení odpovědnosti a rozhodovací pravomoci na straně objednatele
Nezajištění fyzického nebo elektronického přístupu k systémům	Nízké	Včasné otevření komunikace o přístupech a všech nutných podmínkách
Nezajištění všech nutných přístupových oprávnění (účtů) k systémům	Nízké	Zajistit včasnou validaci všech účtů a oprávnění nutných pro provedení převzetí i následné poskytování služby
Nesprávné kontakty v komunikační matici	Nízké	Zajistit včasnou validaci všech kontaktů nutných pro provedení převzetí i následné poskytování služby
Chybějící návaznost na ostatní služby a chybějící kontakt pro případ potřeby.	Nízké	Ověřit všechny vazby ostatních služeb na infrastrukturu. Zajistit a validovat kontakty u všech navazujících služeb, které budou v případě potřeby spolupracovat
Systémy bez podpory	Střední	Zajištění základní servisní podpory provozovaných systémů

KL02 – Monitoring a dohledové služby

Popis návrhu převzetí služeb

Před převzetím služby je nutné nejdříve stanovit jasný plán převzetí. Tento plán musí obsahovat: Vymezení hlavních kontaktních osob, definice procesů, způsob omezování rizik, definice akceptačních kritérií a harmonogram převzetí služeb.

Následně bude nutné jasně specifikovat procesy v rámci převzetí služeb, a to zejména v oblasti kontroly změn, kontroly sporných skutečností a kontroly rizik v převzetí služby. Dále bude nutné vytvořit komunikační matici pro nastavení komunikačních kanálů v této oblasti pro zajištění informovanosti při přebíracím období. V rámci přebíracího období bude definován popis Implementačních kritérií, procesu testování a akceptace připravenosti na započetí poskytování Cílových služeb. Při převzetí služeb bude zohledněn dopady na zaměstnance koncového Zákazníka, dopad na interní procesy a postupy koncového Zákazníka, připravenost vybavení, rozhraní a procesů nutných pro bezproblémové zahájení poskytování Cílových služeb, finanční a obchodní dopady zahájení poskytování Cílových služeb.

Před převzetím služby je nejprve nutné provést analýzu současného stavu dohledového systému. Znamená to, že je nutné zajistit kompletní informace o nastavených procesech v rámci dohledových služeb, komunikačních a eskalačních kontaktech a seznam technických garantů za jednotlivé monitorované skupiny.

Dále je nutné dodat kompletní seznam všech požadovaných monitorovaných zařízení v prostředí Zadavatele s technickým popisem zařízení a provést detailní kontrolu, zda požadované zařízení je obsahem současného dohledového nástroje. V případě, že požadované zařízení nebude obsahem současného dohledového nástroje, bude nutné vypracovat harmonogram jednotlivých činností pro kompletaci uvedené konfigurace. Dále bude provedena kontrola monitorování jednotlivých služeb na zařízení, kontrola přiřazených kontaktů a kontrola nastavených notifikací.

Během převzetí uvedené služby bude vypracována zpráva, ve které budou uvedeny zjištěné skutečnosti během přebíracího období a zároveň návrh činností pro zkvalitnění dodávané služby.

Před zahájením spuštění uvedení služby, bude prezentován stav převzetí služby s reálnou ukázkou dohledového nástroje, navrhnutých procesů a doporučení pro zadavatele.

Před samotným zahájením plněním služby musí proběhnout akceptace této části, kde budou uvedeny veškeré detaily z průběhu analýzy a potvrzeny navrhnuté procesy.

Po této akceptaci dojde k plnohodnotnému poskytování uvedené služby a zahájeno reportování a plní SLA parametrů.

Přístup k řešení dané oblasti

Převzetí uvedené služby bude stanoveno dle standardních využívaných metodik a v závislosti na poskytovaných službách tak, aby nedošlo k omezení poskytovaných služeb a zároveň aby služba byla převzata s veškerými důležitými závislostmi na další poskytované služby a aby nedošlo k omezení těchto služeb během přebíracího období.

Oblast poskytování uvedené služby Monitoring a dohledové služby je závislé na Obecné pravidelné služby a SLA, HelpDesk služby, Správa serverové výpočetní infrastruktury SUN Sparc, SUN Enterprise, Správa serverové výpočetní infrastruktury IBM x86, Správa serverové výpočetní infrastruktury IBM POWER, Správa serverové výpočetní infrastruktury HPe, Správa prostředí Managementu, SAN a diskových polí, Správa LAN prvků DC, Správa virtualizační

platformy VMware, Správa služby MS Active Directory, Správa služby Certifikační autorita, Správa databázových serverů pro ORACLE, Správa databázových serverů pro MS SQL, Správa databázových serverů pro INFORMIX, Správa služby MS Exchange Server, Správa MS Windows serverů a Linux serverů.

V rámci monitoringu jednotlivých zařízení je nutné provádět konfigurace na monitorovacích nástrojů.

V rámci přebíracího období musí být jasně specifikovány měřitelné parametry dle katalogového listu, pro zajištění vyhodnocování těchto služeb. Jednotlivé parametry SLA budou vyhodnocovány přímo z dohledového nástroje, který tyto parametry eviduje. Tyto měřitelné hodnoty bude obsahovat pravidelný report, který bude obsahovat uvedené hodnoty a tím i informace o plnění uvedené služby.

Metodický a procesní postup převzetí služeb

Pro zajištění převzetí uvedené služby bude použita projektová metodika PRINCE2® dle které budou zajištěny veškeré náležitosti, jako jsou:

- Celkové naplánování převzetí služby – seznam dílčích kroků, jejich vzájemných vazeb a termínů zahájení a ukončení
- Definice rizik v převzetí služby
- Koordinace třetích stran a optimalizovat potřebné součinnosti při převzetí služby

Převzetí služby bude dále probíhat dle metodiky ITIL, která zajistí převzetí požadovaných služeb dle definovaných standardů. Použitá metodika bude řešit zejména níže uvedené oblasti.

- Definice požadované služby
- Nastavení služby
- Testovací provoz služby
- Validace služby
- Řízení změn
- Měření služby

Při převzetí služeb je nutné zohlednění metodik a politik v prostředí Zadavatele, a to zejména vydaných metodických pokynů a jednotlivých provozních řádů. Konkrétně se jedná o:

- Politika bezpečnosti informací Magistrátu hl. m. Prahy
- Technická bezpečnostní politika správy ICT
- Technická bezpečnostní politika sítí
- Technická bezpečnostní politika konfigurace ICT
- Instrukce pro přístup do oblastí zajištěných PZTS
- Metodický pokyn č. 7/2017–k řízení bezpečnostních událostí a bezpečnostních incidentů
- Metodický pokyn č. 8/2017 - Pravidla užívání informačního systému Magistrátu hl. m. Prahy
- Metodický pokyn č. 2/2018–k systému řízení IT služeb
- Metodický pokyn č. 1/2019 – Provozní řád datového centra DC4
- Metodický pokyn č. 2/2019 – Provozní řád datového centra DC5

Návrh harmonogramu

Detail činnosti	T+3	T+8	T+12	T+14	T+18
Příprava plánu převzetí					
Předání a seznámení se s dokumentací					
Předání seznamu všech monitorovaných prvků					
Převzetí administrátorských přístupů					
Provedení analýzy prostředí					
Kontrola současného nastavení dohledového nástroje					
Příprava reportu za uvedenou službu					
Workshop před převzetím služby					
Převzetí služby					

(T=počty dnů)

Požadovaná součinnost zadavatele

Pro převzetí služby bude nutné od zadavatele zajistit následující body:

- Nastavení fyzického i elektronického přístupu k dotčeným systémům pro poskytovatele
- Dodání dokumentace prostředí související infrastruktury, seznamu souvisejícího HW a SW
- Nastavení kontaktních a zodpovědných osob do kontaktní matice, a to včetně kontaktů pro komunikaci s dalšími navazujícími službami
- Jednotlivé procesy a postupy pro dohled prostředí
- Seznam všech prvků, které mají být monitorovány (IP adresy)
- Definice kritických systémů
- Požadované notifikační schéma a seznam kontaktů pro notifikace
- Přidělení administrátorského přístupu do dohledovému systému správcům
- Dodání přístupových oprávnění ke všem příslušným systémům
- Zajištění VPN připojení

V rámci převzetí uvedené služby, nejsou potřeba detailní technické znalosti zadavatele. Předpokládaná součinnost zadavatele by neměla přesáhnout pracnost 2 MD.

Analýza rizik v dané oblasti

V rámci analýzy a řízení rizik je potřeba postupovat následujícími kroky „Identifikace" -> „Hodnocení" -> „Implementace". Analýza rizik je prováděna dle odhadnuté pravděpodobnosti a dopadu.

Pro převzetí uvedené služby jsme identifikovaly následující rizika:

Riziko	Hodnocení rizika	Návrh nápravného opatření
Nedodržení časového harmonogramu	Střední	Včasné zajištění veškerých potřebných podkladů a součinností pro převzetí služby
Nedostatečný přístup k informacím pro provedení	Střední	Včasné předání veškerých potřebných informací a

analýzy		přístupů pro provedení analýzy, správné nastavení komunikační matice
Nedostatečná nebo žádná dokumentace k systémům	Střední	Zajistit podporu objednatele, stanovení odpovědnosti na straně objednatele a zajištění potřebných vstupů. Detailní validace dokumentace vůči skutečnosti.
Poškození dat	Nízké	Pro minimalizování rizika je nutné mít zajištěny zálohy dohledového systému
Nesoučinnost třetích stran	Střední	Včasné kontaktování třetích stran pro zajištění potřebných součinností, stanovení odpovědnosti a rozhodovací pravomoci na straně objednatele
Nezajištění fyzického nebo elektronického přístupu k systémům	Nízké	Včasné otevření komunikace o přístupech a všech nutných podmínkách
Nezajištění všech nutných přístupových oprávnění (účtů) k systémům	Nízké	Zajistit včasnou validaci všech účtů a oprávnění nutných pro provedení převzetí i následné poskytování služby
Nesprávné kontakty v komunikační matici	Nízké	Zajistit včasnou validaci všech kontaktů nutných pro provedení převzetí i následné poskytování služby
Chybějící návaznost na ostatní služby a chybějící kontakt pro případ potřeby.	Nízké	Ověřit všechny vazby ostatních služeb na infrastrukturu. Zajistit a validovat kontakty u všech navazujících služeb, které budou v případě potřeby spolupracovat
Nekompletní seznam monitorovaných systémů	Střední	Kompletace seznamu všech zařízení, které mají být monitorovány

KL03 – HelpDesk služby

Popis návrhu převzetí služeb

Před převzetím služby je nutné nejdříve stanovit jasný plán převzetí. Tento plán musí obsahovat: Vymezení hlavních kontaktních osob, definice procesů, způsob omezování rizik, definice akceptačních kritérií a harmonogram převzetí služeb.

Následně bude nutné jasně specifikovat procesy v rámci převzetí služeb, a to zejména v oblasti kontroly změn, kontroly sporných skutečností a kontroly rizik v převzetí služby. Dále bude nutné vytvořit komunikační matici pro nastavení komunikačních kanálů v této oblasti pro zajištění informovanosti při přebíracím období. V rámci přebíracího období bude definován popis Implementačních kritérií, procesu testování a akceptace připravenosti na započetí poskytování Cílových služeb. Při převzetí služeb bude zohledněn dopady na zaměstnance koncového Zákazníka, dopad na interní procesy a postupy koncového Zákazníka, připravenost vybavení, rozhraní a procesů nutných pro bezproblémové zahájení poskytování Cílových služeb, finanční a obchodní dopady zahájení poskytování Cílových služeb.

Pro převzetí uvedené služby je nutné analyzovat současný stav a nastavených procesů. To znamená provést kontrolu všech nastavených pravidel, kategorií, kontaktů, oprávnění a návazných procesů. Nedílnou součástí musí být kontrola nastavených parametrů SLA pro jednotlivé kategorie. Zároveň musí být provedena kontrola nastavení parametrů v rámci zajištění podpory 24/7.

Po provedení této analýzy musí být zahájena příprava prostředí pro spuštění služby. To znamená vytvoření helpdeskového prostředí, nadefinování potřebných kategorií a skupiny dle provedené analýzy a dle poskytovaných služeb a nadefinování uživatelského prostředí.

Po tomto nastavení musí proběhnout test veškerých funkcionalit ze strany zadavatele. Následně musí být ze strany dodavatele připraveno helpdeskové centrum, operátorům musí být předána kontaktní matice za jednotlivé systémy pro plnění služby v režimu 24/7 a informováni operátoři o spuštění služby.

Po provedeném testu bude připravena prezentace helpdeskové služby, navrhnutých procesů a zároveň ukázka reportování uvedené služby. Po tomto kroku bude předložen akceptační protokol s uvedenými skutečnostmi. Po akceptaci musí dojít k informování uživatelů a všech dotčených subjektů o změně této služby a termínu spuštění služby.

Po těchto krocích může dojít ke spuštění této služby.

Přístup k řešení dané oblasti

Převzetí uvedené služby bude stanoveno dle standardních využívaných metodik a v závislosti na poskytovaných službách tak, aby nedošlo k omezení poskytovaných služeb a zároveň aby služba byla převzata s veškerými důležitými závislostmi na další poskytované služby a aby nedošlo k omezení těchto služeb během přebíracího období.

Oblast poskytování uvedené služby je závislé na obecných a pravidelných službách SLA a dohledového systému. Naopak tuto službu využívají ostatní katalogové listy, pro které je služba Helpdesku využívána jako jednotné místo pro evidenci požadavků.

V rámci přebíracího období musí být jasně specifikovány měřitelné parametry dle katalogového listu, pro zajištění vyhodnocování těchto služeb. Jednotlivé parametry SLA budou vyhodnocovány z helpdeskového nástroje, který tyto parametry eviduje. Tyto měřitelné hodnoty bude obsahovat pravidelný report, který bude obsahovat uvedené hodnoty a tím i informace o plnění uvedené služby.

Metodický a procesní postup převzetí služeb

Pro zajištění převzetí uvedené služby bude použita projektová metodika PRINCE2® dle které budou zajištěny veškeré náležitosti, jako jsou:

- Celkové naplánování převzetí služby – seznam dílčích kroků, jejich vzájemných vazeb a termínů zahájení a ukončení
- Definice rizik v převzetí služby
- Koordinace třetích stran a optimalizovat potřebné součinnosti při převzetí služby

Převzetí služby bude dále probíhat dle metodiky ITIL, která zajistí převzetí požadovaných služeb dle definovaných standardů. Použitá metodika bude řešit zejména níže uvedené oblasti.

- Definice požadované služby
- Nastavení služby
- Testovací provoz služby
- Validace služby
- Řízení změn
- Měření služby

Při převzetí služeb je nutné zohlednění metodik a politik v prostředí Zadavatele, a to zejména vydaných metodických pokynů a jednotlivých provozních řádů. Konkrétně se jedná o:

- Politika bezpečnosti informací Magistrátu hl. m. Prahy
- Technická bezpečnostní politika správy ICT
- Technická bezpečnostní politika sítí
- Technická bezpečnostní politika konfigurace ICT
- Instrukce pro přístup do oblastí zajištěných PZTS
- Metodický pokyn č. 7/2017–k řízení bezpečnostních událostí a bezpečnostních incidentů
- Metodický pokyn č. 8/2017 - Pravidla užívání informačního systému Magistrátu hl. m. Prahy
- Metodický pokyn č. 2/2018–k systému řízení IT služeb
- Metodický pokyn č. 1/2019 – Provozní řád datového centra DC4
- Metodický pokyn č. 2/2019 – Provozní řád datového centra DC5

Návrh harmonogramu

Detail činnosti	T+2	T+6	T+10	T+12	T+13	T+16

Příprava plánu převzetí						
Předání a seznámení se s dokumentací						
Provedení analýzy prostředí						
Prověření nastavených procesů						
Příprava prostředí helpdesk						
Test nastavení a přístupů						
Workshop před převzetím služby						
Informování uživatelů o změně služby						
Převzetí služby						

(T=počty dnů)

Požadovaná součinnost zadavatele

- Seznam kategorií pro evidenci požadavků
- Seznam procesů, eskalačních matic a jednotlivých kontaktů
- Seznam uživatelů s přístupem do helpdeskového nástroje (jméno, příjmení a emailová adresa)
- Stanovení vzoru pravidelného reportingu

Požadovaná součinnost by neměla přesáhnout pracnost 2 MD

Analýza rizik v dané oblasti

V rámci analýzy a řízení rizik je potřeba postupovat následujícími kroky „Identifikace" -> „Hodnocení" -> „Implementace". Analýza rizik je prováděna dle odhadnuté pravděpodobnosti a dopadu.

Pro převzetí uvedené služby jsme identifikovaly následující rizika:

Riziko	Hodnocení rizika	Návrh nápravného opatření
Nedodržení časového harmonogramu	Střední	Včasné zajištění veškerých potřebných podkladů a součinností pro převzetí služby
Nedostatečný přístup k informacím pro provedení analýzy	Střední	Včasné předání veškerých potřebných informací a přístupů pro provedení analýzy, správné nastavení komunikační matice
Nedostatečná nebo žádná dokumentace k systémům	Střední	Zajistit podporu objednatele, stanovení odpovědnosti na straně objednatele a zajištění potřebných vstupů. Detailní validace dokumentace vůči skutečnosti.
Poškození dat	Střední	Pro minimalizování rizika je nutné mít zajištěny zálohy

		dohledového systému
Nesoučinnost třetích stran	Střední	Včasné kontaktování třetích stran pro zajištění potřebných součinností, stanovení odpovědnosti a rozhodovací pravomoci na straně objednatele
Nesprávné kontakty v komunikační matici	Nízké	Zajistit včasnou validaci všech kontaktů nutných pro provedení převzetí i následné poskytování služby
Chybějící návaznost na ostatní služby a chybějící kontakt pro případ potřeby.	Nízké	Ověřit všechny vazby ostatních služeb. Zajistit a validovat kontakty u všech navazujících služeb, které budou v případě potřeby spolupracovat

KL04a – Správa serverové výpočetní infrastruktury SUN Sparc, SUN Enterprise

Popis návrhu převzetí služeb

Před převzetím služby je nutné nejdříve stanovit jasný plán převzetí. Tento plán musí obsahovat: Vymezení hlavních kontaktních osob, definice procesů, způsob omezování rizik, definice akceptačních kritérií a harmonogram převzetí služeb.

Následně bude nutné jasně specifikovat procesy v rámci převzetí služeb, a to zejména v oblasti kontroly změn, kontroly sporných skutečností a kontroly rizik v převzetí služby. Dále bude nutné vytvořit komunikační matici pro nastavení komunikačních kanálů v této oblasti pro zajištění informovanosti při přebíracím období. V rámci přebíracího období bude definován popis Implementačních kritérií, procesu testování a akceptace připravenosti na započetí poskytování Cílových služeb. Při převzetí služeb bude zohledněn dopady na zaměstnance koncového Zákazníka, dopad na interní procesy a postupy koncového Zákazníka, připravenost vybavení, rozhraní a procesů nutných pro bezproblémové zahájení poskytování Cílových služeb, finanční a obchodní dopady zahájení poskytování Cílových služeb.

Při převzetí služby je nejprve nutné provést analýzu této oblasti. Je nutné zajistit detailní dokumentaci k danému prostředí, zejména je nutné zajistit kompletní seznam HW, který bude obsahovat detailní popis HW a komponent, jejich umístění, výrobní čísla HW, verze mikrokódů jednotlivých HW, stavy záruk jednotlivých zařízení, seznam administrátorských přístupů, seznam provozovaných systémů na tomto HW a seznam kontaktů zodpovědných za dané systémy. Nedílnou součástí této analýzy by mělo být dodání ze strany zadavatele vazeb HW na jednotlivé aplikace z pohledu celé architektury prostředí.

Předpokladem je dokumentace, obsahující následující informace:

- Jednotlivé serverové technologie jejich označení model/typ/sériové číslo
- HW konfigurace serverů
- Verze mikrokódů (FW) serveru
- IP adresy managementu serveru a přístupové údaje
- Instalovaný OS, IP adresa OS a přístupové údaje
- V případě hypervizoru, rozpis jednotlivých virtuálních serverů
- Virtuální serverová infrastruktura – popis každého serveru, jeho konfigurace po stránce HW tak SW a přístupové údaje
- Záruky na servery

Po dodání těchto informací musí dojít k fyzického kontrole uvedeného HW, a to jak po stránce vizuální, tak i přihlášením na tento HW.

Po uvedené analýze musí dojít k vytvoření nových administrátorských přístupů pro možnost správy HW a odebrání původních přístupů.

Následně budou převzaté systémy zaneseny do dokumentace, připraven návrh pravidelných zásahů na HW (update mikrokódů), zajištěno monitorování HW a nastavení SLA parametrů pro definovaný HW.

Během převzetí uvedené služby bude vypracována zpráva, ve které budou uvedeny zjištěné skutečnosti během přebíracího období a zároveň návrh činností pro zkvalitnění dodávané služby.

Po tomto kroku bude předložen akceptační protokol s uvedenými skutečnostmi z přebíracího období.

Následně dojde ke spuštění služby a zároveň k zahájení měření jednotlivých SLA parametrů, které budou pravidelně reportovány.

Přístup k řešení dané oblasti

Převzetí uvedené služby bude stanoveno dle standardních využívaných metodik a v závislosti na poskytovaných službách tak, aby nedošlo k omezení poskytovaných služeb a zároveň aby služba byla převzata s veškerými důležitými závislostmi na další poskytované služby a aby nedošlo k omezení těchto služeb během přebíracího období.

Oblast poskytování uvedené služby Správa serverové výpočetní infrastruktury SUN Sparc, SUN Enterprise je závislé na Obecné pravidelné služby a SLA, Monitoring a dohledový systém, HelpDesk služby, Správa prostředí Managementu, SAN a diskových polí, Správa LAN prvků DC, Správa virtualizační platformy VMware, Správa služby MS Active Directory, Správa infrastrukturních služeb, Správa databázových serverů pro ORACLE, Správa databázových serverů pro MS SQL, Správa databázových serverů pro INFORMIX, Správa MS Windows serverů a Linux serverů.

V rámci přebíracího období musí být jasně specifikovány měřitelné parametry dle katalogového listu, pro zajištění vyhodnocování této služby. Jednotlivé parametry SLA budou vyhodnocovány z dohledového nástroje, který tyto parametry eviduje. Tyto měřitelné

hodnoty bude obsahovat pravidelný report, ve kterém budou uvedené hodnoty a tím i informace o plnění uvedené služby.

Metodický a procesní postup převzetí služeb

Pro zajištění převzetí uvedené služby bude použita projektová metodika PRINCE2® dle které budou zajištěny veškeré náležitosti, jako jsou:

- Celkové naplánování převzetí služby – seznam dílčích kroků, jejich vzájemných vazeb a termínů zahájení a ukončení.
- Definice rizik v převzetí služby
- Koordinace třetích stran a optimalizovat potřebné součinnosti při převzetí služby.

Převzetí služby bude dále probíhat dle metodiky ITIL, která zajistí převzetí požadovaných služeb dle definovaných standardů. Použitá metodika bude řešit zejména níže uvedené oblasti.

- Definice požadované služby
- Nastavení služby
- Testovací provoz služby
- Validace služby
- Řízení změn
- Měření služby

Při převzetí služeb je nutné zohlednění metodik a politik v prostředí Zadavatele, a to zejména vydaných metodických pokynů a jednotlivých provozních řádů.
Konkrétně se jedná o:

- Politika bezpečnosti informací Magistrátu hl. m. Prahy
- Technická bezpečnostní politika správy ICT
- Technická bezpečnostní politika sítí
- Technická bezpečnostní politika konfigurace ICT
- Instrukce pro přístup do oblastí zajištěných PZTS
- Metodický pokyn č. 7/2017–k řízení bezpečnostních událostí a bezpečnostních incidentů
- Metodický pokyn č. 8/2017 - Pravidla užívání informačního systému Magistrátu hl. m. Prahy
- Metodický pokyn č. 2/2018–k systému řízení IT služeb
- Metodický pokyn č. 1/2019 – Provozní řád datového centra DC4
- Metodický pokyn č. 2/2019 – Provozní řád datového centra DC5

Návrh harmonogramu

Detail činnosti	T+3	T+5	T+10	T+12	T+16	T+18	T+20
Příprava plánu převzetí							
Předání a seznámení se s dokumentací							
Provedení analýzy prostředí							
Ověření stavu záruk							
Kontrola jednotlivých prvků							

Nastavení oprávnění na prvky							
Nastavení návazných procesů - monitoring							
Workshop před převzetím služby							
Převzetí služby							

(T=počty dnů)

Požadovaná součinnost zadavatele

- Seznam fyzických serverů a jejich umístění
- Detailní informace ke každému serveru
  - kompletní konfigurace všech součástí serverů
  - stavy záruk
  - Verze instalovaného operačního systému
  - Přístupové oprávnění na management těchto serverů
- Seznam aplikací, které jsou provozovány na serverech a seznam administrátorů zodpovědných za aplikace
- Nastavení fyzického i elektronického přístupu k dotčeným systémům pro poskytovatele
- Dodání dokumentace a veškeré související infrastruktury, seznamu souvisejícího HW a SW
- Nastavení kontaktních a zodpovědných osob do kontaktní matice, a to včetně kontaktů pro komunikaci s dalšími navazujícími službami
- Dodání přístupových oprávnění ke všem příslušným systémům
- Stanovení vzoru pravidelného reportingu
- Zajištění VPN připojení

Požadovaná součinnost by neměla přesáhnout pracnost 3 MD

Analýza rizik v dané oblasti

V rámci analýzy a řízení rizik je potřeba postupovat následujícími kroky „Identifikace" -> „Hodnocení" -> „Implementace". Analýza rizik je prováděna dle odhadnuté pravděpodobnosti a dopadu.

Pro převzetí uvedené služby jsme identifikovaly následující rizika:

Riziko	Hodnocení rizika	Návrh nápravného opatření
Nedodržení časového harmonogramu	Střední	Včasné zajištění veškerých potřebných podkladů a součinností pro převzetí služby
Nedostatečný přístup k informacím pro provedení analýzy	Střední	Včasné předání veškerých potřebných informací a přístupů pro provedení analýzy, správné nastavení komunikační matice
Nedostatečná nebo žádná dokumentace k systémům	Střední	Zajistit podporu objednatele, stanovení odpovědnosti na straně objednatele a zajištění

		potřebných vstupů. Detailní validace dokumentace vůči skutečnosti.
Poškození dat	Střední	Pro minimalizování rizika je nutné mít zajištěny zálohy dohledového systému
Nesoučinnost třetích stran	Střední	Včasné kontaktování třetích stran pro zajištění potřebných součinností, stanovení odpovědnosti a rozhodovací pravomoci na straně objednatele
Nezajištění fyzického nebo elektronického přístupu k systémům	Nízké	Včasné otevření komunikace o přístupech a všech nutných podmínkách
Nezajištění všech nutných přístupových oprávnění (účtů) k systémům	Nízké	Zajistit včasnou validaci všech účtů a oprávnění nutných pro provedení převzetí i následné poskytování služby
Nesprávné kontakty v komunikační matici	Nízké	Zajistit včasnou validaci všech kontaktů nutných pro provedení převzetí i následné poskytování služby
Chybějící návaznost na ostatní služby a chybějící kontakt pro případ potřeby.	Nízké	Ověřit všechny vazby ostatních služeb na infra SUN Sparc. Zajistit a validovat kontakty u všech navazujících služeb, které budou v případě potřeby spolupracovat
Systémy bez podpory	Vysoké	Zajištění základní servisní podpory provozovaných systémů
Nepodporované verze mikrokódů	Střední	Zajištění aktualizace verze mikrokódů na podporovanou verzi výrobce

KL04b – Správa serverové výpočetní infrastruktury IBM x86

Popis návrhu převzetí služeb

Před převzetím služby je nutné nejdříve stanovit jasný plán převzetí. Tento plán musí obsahovat: Vymezení hlavních kontaktních osob, definice procesů, způsob omezování rizik, definice akceptačních kritérií a harmonogram převzetí služeb.

Následně bude nutné jasně specifikovat procesy v rámci převzetí služeb, a to zejména v oblasti kontroly změn, kontroly sporných skutečností a kontroly rizik v převzetí služby. Dále bude nutné vytvořit komunikační matici pro nastavení komunikačních kanálů v této oblasti pro zajištění informovanosti při přebíracím období. V rámci přebíracího období bude definován popis Implementačních kritérií, procesu testování a akceptace připravenosti na započetí poskytování Cílových služeb. Při převzetí služeb bude zohledněn dopady na zaměstnance koncového Zákazníka, dopad na interní procesy a postupy koncového Zákazníka, připravenost vybavení, rozhraní a procesů nutných pro bezproblémové zahájení poskytování Cílových služeb, finanční a obchodní dopady zahájení poskytování Cílových služeb.

Při převzetí služby je nejprve nutné provést analýzu této oblasti. Je nutné zajistit detailní dokumentaci k danému prostředí, zejména je nutné zajistit kompletní seznam HW, který bude obsahovat detailní popis HW a komponent, jejich umístění, výrobní čísla HW, verze mikrokódů jednotlivých HW, stavy záruk jednotlivých zařízení, seznam administrátorských přístupů, seznam provozovaných systémů na tomto HW a seznam kontaktů zodpovědných za dané systémy. Nedílnou součástí této analýzy by mělo být dodání ze strany zadavatele vazeb HW na jednotlivé aplikace z pohledu celé architektury prostředí.

Předpokladem je dokumentace, obsahující následující informace:

- Jednotlivé serverové technologie jejich označení model/typ/sériové číslo
- HW konfigurace serverů
- Verze mikrokódů (FW) serveru
- IP adresy managementu serveru a přístupové údaje
- Instalovaný OS, IP adresa OS a přístupové údaje
- V případě hypervizoru, rozpis jednotlivých virtuálních serverů
- Virtuální serverová infrastruktura – popis každého serveru, jeho konfigurace po stránce HW tak SW a přístupové údaje
- Záruky na servery

Po dodání těchto informací musí dojít k fyzického kontrole uvedeného HW, a to jak po stránce vizuální, tak i přihlášením na tento HW.

Po uvedené analýze musí dojít k vytvoření nových administrátorských přístupů pro možnost správy HW a odebrání původních přístupů.

Následně budou převzaté systémy zaneseny do dokumentace, připraven návrh pravidelných zásahů na HW (update mikrokódů), zajištěno monitorování HW a nastavení SLA parametrů pro definovaný HW.

Během převzetí uvedené služby bude vypracována zpráva, ve které budou uvedeny zjištěné skutečnosti během přebíracího období a zároveň návrh činností pro zkvalitnění dodávané služby.

Po tomto kroku bude předložen akceptační protokol s uvedenými skutečnostmi z přebíracího období.

Následně dojde ke spuštění služby a zároveň k zahájení měření jednotlivých SLA parametrů, které budou pravidelně reportovány.

Přístup k řešení dané oblasti

Převzetí uvedené služby bude stanoveno dle standardních využívaných metodik a v závislosti na poskytovaných službách tak, aby nedošlo k omezení poskytovaných služeb a zároveň aby služba byla převzata s veškerými důležitými závislostmi na další poskytované služby a aby nedošlo k omezení těchto služeb během přebíracího období.

Oblast poskytování uvedené služby Správa serverové výpočetní infrastruktury IBM x86 je závislé na Obecné pravidelné služby a SLA, Monitoring a dohledový systém, HelpDesk služby, Správa prostředí Managementu, SAN a diskových polí, Správa LAN prvků DC, Správa virtualizační platformy VMware, Správa služby MS Active Directory, Správa infrastrukturních služeb, Správa databázových serverů pro ORACLE, Správa databázových serverů pro MS SQL, Správa databázových serverů pro INFORMIX, Správa MS Windows serverů a Linux serverů.

V rámci přebíracího období musí být jasně specifikovány měřitelné parametry dle katalogového listu, pro zajištění vyhodnocování této služby. Jednotlivé parametry SLA budou vyhodnocovány z dohledového nástroje, který tyto parametry eviduje. Tyto měřitelné hodnoty bude obsahovat pravidelný report, ve kterém budou uvedené hodnoty a tím i informace o plnění uvedené služby.

Metodický a procesní postup převzetí služeb

Pro zajištění převzetí uvedené služby bude použita projektová metodika PRINCE2® dle které budou zajištěny veškeré náležitosti, jako jsou:

- Celkové naplánování převzetí služby – seznam dílčích kroků, jejich vzájemných vazeb a termínů zahájení a ukončení
- Definice rizik v převzetí služby
- Koordinace třetích stran a optimalizovat potřebné součinnosti při převzetí služby

Převzetí služby bude dále probíhat dle metodiky ITIL, která zajistí převzetí požadovaných služeb dle definovaných standardů. Použitá metodika bude řešit zejména níže uvedené oblasti.

- Definice požadované služby
- Nastavení služby
- Testovací provoz služby
- Validace služby
- Řízení změn
- Měření služby

Při převzetí služeb je nutné zohlednění metodik a politik v prostředí Zadavatele, a to zejména vydaných metodických pokynů a jednotlivých provozních řádů. Konkrétně se jedná o:

- Politika bezpečnosti informací Magistrátu hl. m. Prahy
- Technická bezpečnostní politika správy ICT
- Technická bezpečnostní politika sítí
- Technická bezpečnostní politika konfigurace ICT
- Instrukce pro přístup do oblastí zajištěných PZTS

- Metodický pokyn č. 7/2017–k řízení bezpečnostních událostí a bezpečnostních incidentů
- Metodický pokyn č. 8/2017 - Pravidla užívání informačního systému Magistrátu hl. m. Prahy
- Metodický pokyn č. 2/2018–k systému řízení IT služeb
- Metodický pokyn č. 1/2019 – Provozní řád datového centra DC4
- Metodický pokyn č. 2/2019 – Provozní řád datového centra DC5

Návrh harmonogramu

Detail činnosti	T+3	T+5	T+10	T+12	T+16	T+18	T+20
Příprava plánu převzetí							
Předání a seznámení se s dokumentací							
Provedení analýzy prostředí							
Ověření stavu záruk							
Kontrola jednotlivých prvků							
Nastavení oprávnění na prvky							
Nastavení návazných procesů - monitoring							
Workshop před převzetím služby							
Převzetí služby							

(T=počty dnů)

Požadovaná součinnost zadavatele

- Seznam fyzických serverů a jejich umístění
- Detailní informace ke každému serveru
  - kompletní konfigurace všech součástí serverů
  - stavy záruk
  - Verze instalovaného operačního systému
  - Přístupové oprávnění na management těchto serverů
- Seznam aplikací, které jsou provozovány na serverech a seznam administrátorů zodpovědných za aplikace
- Nastavení fyzického i elektronického přístupu k dotčeným systémům pro poskytovatele
- Dodání dokumentace a veškeré související infrastruktury, seznamu souvisejícího HW a SW
- Nastavení kontaktních a zodpovědných osob do kontaktní matice, a to včetně kontaktů pro komunikaci s dalšími navazujícími službami
- Dodání přístupových oprávnění ke všem příslušným systémům
- Stanovení vzoru pravidelného reportingu
- Zajištění VPN připojení

Požadovaná součinnost by neměla přesáhnout pracnost 3 MD

Analýza rizik v dané oblasti

V rámci analýzy a řízení rizik je potřeba postupovat následujícími kroky „Identifikace" -> „Hodnocení" -> „Implementace". Analýza rizik je prováděna dle odhadnuté pravděpodobnosti a dopadu.

Pro převzetí uvedené služby jsme identifikovaly následující rizika:

Riziko	Hodnocení rizika	Návrh nápravného opatření
Nedodržení časového harmonogramu	Střední	Včasné zajištění veškerých potřebných podkladů a součinností pro převzetí služby
Nedostatečný přístup k informacím pro provedení analýzy	Střední	Včasné předání veškerých potřebných informací a přístupů pro provedení analýzy, správné nastavení komunikační matice
Nedostatečná nebo žádná dokumentace k systémům	Střední	Zajistit podporu objednatele, stanovení odpovědnosti na straně objednatele a zajištění potřebných vstupů. Detailní validace dokumentace vůči skutečnosti.
Poškození dat	Střední	Pro minimalizování rizika je nutné mít zajištěny zálohy dohledového systému
Nesoučinnost třetích stran	Střední	Včasné kontaktování třetích stran pro zajištění potřebných součinností, stanovení odpovědnosti a rozhodovací pravomoci na straně objednatele
Nezajištění fyzického nebo elektronického přístupu k systémům	Nízké	Včasné otevření komunikace o přístupech a všech nutných podmínkách
Nezajištění všech nutných přístupových oprávnění (účtů) k systémům	Nízké	Zajistit včasnou validaci všech účtů a oprávnění nutných pro provedení převzetí i následné poskytování služby
Nesprávné kontakty v komunikační matici	Nízké	Zajistit včasnou validaci všech kontaktů nutných pro provedení převzetí i následné poskytování služby
Chybějící návaznost na ostatní služby a chybějící kontakt pro případ potřeby.	Nízké	Ověřit všechny vazby ostatních služeb na infra SUN Sparc. Zajistit a validovat kontakty u všech navazujících služeb, které budou v případě

		potřeby spolupracovat
Systémy bez podpory	Vysoké	Zajištění základní servisní podpory provozovaných systémů
Nepodporované verze mikrokódů	Střední	Zajištění aktualizace verze mikrokódů na podporovanou verzi výrobce

KL04c – Správa serverové výpočetní infrastruktury IBM POWER

Popis návrhu převzetí služeb

Před převzetím služby je nutné nejdříve stanovit jasný plán převzetí. Tento plán musí obsahovat: Vymezení hlavních kontaktních osob, definice procesů, způsob omezování rizik, definice akceptačních kritérií a harmonogram převzetí služeb.

Následně bude nutné jasně specifikovat procesy v rámci převzetí služeb, a to zejména v oblasti kontroly změn, kontroly sporných skutečností a kontroly rizik v převzetí služby. Dále bude nutné vytvořit komunikační matici pro nastavení komunikačních kanálů v této oblasti pro zajištění informovanosti při přebíracím období. V rámci přebíracího období bude definován popis Implementačních kritérií, procesu testování a akceptace připravenosti na započetí poskytování Cílových služeb. Při převzetí služeb bude zohledněn dopady na zaměstnance koncového Zákazníka, dopad na interní procesy a postupy koncového Zákazníka, připravenost vybavení, rozhraní a procesů nutných pro bezproblémové zahájení poskytování Cílových služeb, finanční a obchodní dopady zahájení poskytování Cílových služeb.

Při převzetí služby je nejprve nutné provést analýzu této oblasti. Je nutné zajistit detailní dokumentaci k danému prostředí, zejména je nutné zajistit kompletní seznam HW, který bude obsahovat detailní popis HW a komponent, jejich umístění, výrobní čísla HW, verze mikrokódů jednotlivých HW, stavy záruk jednotlivých zařízení, seznam administrátorských přístupů, seznam provozovaných systémů na tomto HW a seznam kontaktů zodpovědných za dané systémy. Nedílnou součástí této analýzy by mělo být dodání ze strany zadavatele vazeb HW na jednotlivé aplikace z pohledu celé architektury prostředí.

Předpokladem je dokumentace, obsahující následující informace:

- Jednotlivé serverové technologie jejich označení model/typ/sériové číslo
- HW konfigurace serverů
- Verze mikrokódů (FW) serveru
- IP adresy managementu serveru a přístupové údaje
- Instalovaný OS, IP adresa OS a přístupové údaje
- V případě hypervizoru, rozpis jednotlivých virtuálních serverů
- Virtuální serverová infrastruktura – popis každého serveru, jeho konfigurace po stránce HW tak SW a přístupové údaje
- Záruky na servery

Po dodání těchto informací musí dojít k fyzického kontrole uvedeného HW, a to jak po stránce vizuální, tak i přihlášením na tento HW.

Po uvedené analýze musí dojít k vytvoření nových administrátorských přístupů pro možnost správy HW a odebrání původních přístupů.

Následně budou převzaté systémy zaneseny do dokumentace, připraven návrh pravidelných zásahů na HW (update mikrokódů), zajištěno monitorování HW a nastavení SLA parametrů pro definovaný HW.

Během převzetí uvedené služby bude vypracována zpráva, ve které budou uvedeny zjištěné skutečnosti během přebíracího období a zároveň návrh činností pro zkvalitnění dodávané služby.

Po tomto kroku bude předložen akceptační protokol s uvedenými skutečnostmi z přebíracího období.

Následně dojde ke spuštění služby a zároveň k zahájení měření jednotlivých SLA parametrů, které budou pravidelně reportovány.

Přístup k řešení dané oblasti

Převzetí uvedené služby bude stanoveno dle standardních využívaných metodik a v závislosti na poskytovaných službách tak, aby nedošlo k omezení poskytovaných služeb a zároveň aby služba byla převzata s veškerými důležitými závislostmi na další poskytované služby a aby nedošlo k omezení těchto služeb během přebíracího období.

Oblast poskytování uvedené služby Správa serverové výpočetní infrastruktury IBM POWER je závislé na Obecné pravidelné služby a SLA, Monitoring a dohledový systém, HelpDesk služby, Správa prostředí Managementu, SAN a diskových polí, Správa LAN prvků DC, Správa virtualizační platformy VMware, Správa služby MS Active Directory, Správa infrastrukturních služeb, Správa databázových serverů pro ORACLE, Správa databázových serverů pro MS SQL, Správa databázových serverů pro INFORMIX, Správa MS Windows serverů a Linux serverů.

V rámci přebíracího období musí být jasně specifikovány měřitelné parametry dle katalogového listu, pro zajištění vyhodnocování této služby. Jednotlivé parametry SLA budou vyhodnocovány z dohledového nástroje, který tyto parametry eviduje. Tyto měřitelné hodnoty bude obsahovat pravidelný report, ve kterém budou uvedené hodnoty a tím i informace o plnění uvedené služby.

Metodický a procesní postup převzetí služeb

Pro zajištění převzetí uvedené služby bude použita projektová metodika PRINCE2® dle které budou zajištěny veškeré náležitosti, jako jsou:

- Celkové naplánování převzetí služby – seznam dílčích kroků, jejich vzájemných vazeb a termínů zahájení a ukončení
- Definice rizik v převzetí služby
- Koordinace třetích stran a optimalizovat potřebné součinnosti při převzetí služby

Převzetí služby bude dále probíhat dle metodiky ITIL, která zajistí převzetí požadovaných služeb dle definovaných standardů. Použitá metodika bude řešit zejména níže uvedené oblasti.

- Definice požadované služby
- Nastavení služby
- Testovací provoz služby
- Validace služby
- Řízení změn
- Měření služby

Při převzetí služeb je nutné zohlednění metodik a politik v prostředí Zadavatele, a to zejména vydaných metodických pokynů a jednotlivých provozních řádů. Konkrétně se jedná o:

- Politika bezpečnosti informací Magistrátu hl. m. Prahy
- Technická bezpečnostní politika správy ICT
- Technická bezpečnostní politika sítí
- Technická bezpečnostní politika konfigurace ICT
- Instrukce pro přístup do oblastí zajištěných PZTS
- Metodický pokyn č. 7/2017–k řízení bezpečnostních událostí a bezpečnostních incidentů
- Metodický pokyn č. 8/2017 - Pravidla užívání informačního systému Magistrátu hl. m. Prahy
- Metodický pokyn č. 2/2018–k systému řízení IT služeb
- Metodický pokyn č. 1/2019 – Provozní řád datového centra DC4
- Metodický pokyn č. 2/2019 – Provozní řád datového centra DC5

Návrh harmonogramu

Detail činnosti	T+3	T+5	T+10	T+12	T+16	T+18	T+20
Příprava plánu převzetí							
Předání a seznámení se s dokumentací							
Provedení analýzy prostředí							
Ověření stavu záruk							
Kontrola jednotlivých prvků							
Nastavení oprávnění na prvky							
Nastavení návazných procesů - monitoring							
Workshop před převzetím služby							
Převzetí služby							

(T=počty dnů)

Požadovaná součinnost zadavatele

- Nastavení fyzického i elektronického přístupu k dotčeným systémům pro poskytovatele
- Dodání dokumentace prostředí IBM POWER a veškeré související infrastruktury, seznamu souvisejícího HW a SW
- Dodání souhrnu požadovaných provozních parametrů IBM POWER
- Detailní informace ke každému serveru

- kompletní konfigurace všech součástí serverů
- stavy záruk
- Verze instalovaného operačního systému
- Přístupové oprávnění na management těchto serverů

- Seznam aplikací, které jsou provozovány na serverech a seznam administrátorů zodpovědných za aplikace
- Nastavení kontaktních a zodpovědných osob do kontaktní matice, a to včetně kontaktů pro komunikaci s dalšími navazujícími službami
- Dodání přístupových oprávnění ke všem příslušným systémům
- Stanovení vzoru pravidelného reportingu
- Zajištění VPN připojení

Požadovaná součinnost by neměla přesáhnout pracnost 3 MD

Analýza rizik v dané oblasti

V rámci analýzy a řízení rizik je potřeba postupovat následujícími kroky „Identifikace" -> „Hodnocení" -> „Implementace". Analýza rizik je prováděna dle odhadnuté pravděpodobnosti a dopadu.

Pro převzetí uvedené služby jsme identifikovaly následující rizika:

Riziko	Hodnocení rizika	Návrh nápravného opatření
Nedodržení časového harmonogramu	Střední	Včasné zajištění veškerých potřebných podkladů a součinností pro převzetí služby
Nedostatečný přístup k informacím pro provedení analýzy	Střední	Včasné předání veškerých potřebných informací a přístupů pro provedení analýzy, správné nastavení komunikační matice
Nedostatečná nebo žádná dokumentace k systémům	Střední	Zajistit podporu objednatele, stanovení odpovědnosti na straně objednatele a zajištění potřebných vstupů. Detailní validace dokumentace vůči skutečnosti.
Poškození dat	Střední	Pro minimalizování rizika je nutné mít zajištěny zálohy dohledového systému
Nesoučinnost třetích stran	Střední	Včasné kontaktování třetích stran pro zajištění potřebných součinností, stanovení odpovědnosti a rozhodovací pravomoci na straně objednatele
Nezajištění fyzického nebo	Nízké	Včasné otevření komunikace

elektronického přístupu k systémům		o přístupech a všech nutných podmínkách
Nezajištění všech nutných přístupových oprávnění (účtů) k systémům	Nízké	Zajistit včasnou validaci všech účtů a oprávnění nutných pro provedení převzetí i následné poskytování služby
Nesprávné kontakty v komunikační matici	Nízké	Zajistit včasnou validaci všech kontaktů nutných pro provedení převzetí i následné poskytování služby
Chybějící návaznost na ostatní služby a chybějící kontakt pro případ potřeby.	Nízké	Ověřit všechny vazby ostatních služeb na infra SUN Sparc. Zajistit a validovat kontakty u všech navazujících služeb, které budou v případě potřeby spolupracovat
Systémy bez podpory	Vysoké	Zajištění základní servisní podpory provozovaných systémů
Nepodporované verze mikrokódů	Střední	Zajištění aktualizace verze mikrokódů na podporovanou verzi výrobce

KL04d – Správa serverové výpočetní infrastruktury HPe

Popis návrhu převzetí služeb

Před převzetím služby je nutné nejdříve stanovit jasný plán převzetí. Tento plán musí obsahovat: Vymezení hlavních kontaktních osob, definice procesů, způsob omezování rizik, definice akceptačních kritérií a harmonogram převzetí služeb.

Následně bude nutné jasně specifikovat procesy v rámci převzetí služeb, a to zejména v oblasti kontroly změn, kontroly sporných skutečností a kontroly rizik v převzetí služby. Dále bude nutné vytvořit komunikační matici pro nastavení komunikačních kanálů v této oblasti pro zajištění informovanosti při přebíracím období. V rámci přebíracího období bude definován popis Implementačních kritérií, procesu testování a akceptace připravenosti na započetí poskytování Cílových služeb. Při převzetí služeb bude zohledněn dopady na zaměstnance koncového Zákazníka, dopad na interní procesy a postupy koncového Zákazníka, připravenost vybavení, rozhraní a procesů nutných pro bezproblémové zahájení poskytování Cílových služeb, finanční a obchodní dopady zahájení poskytování Cílových služeb.

Při převzetí služby je nejprve nutné provést analýzu této oblasti. Je nutné zajistit detailní dokumentaci k danému prostředí, zejména je nutné zajistit kompletní seznam HW, který bude obsahovat detailní popis HW a komponent, jejich umístění, výrobní čísla HW, verze

mikrokódů jednotlivých HW, stavy záruk jednotlivých zařízení, seznam administrátorských přístupů, seznam provozovaných systémů na tomto HW a seznam kontaktů zodpovědných za dané systémy. Nedílnou součástí této analýzy by mělo být dodání ze strany zadavatele vazeb HW na jednotlivé aplikace z pohledu celé architektury prostředí.

Předpokladem je dokumentace, obsahující následující informace:

- Jednotlivé serverové technologie jejich označení model/typ/sériové číslo
- HW konfigurace serverů
- Verze mikrokódů (FW) serveru
- IP adresy managementu serveru a přístupové údaje
- Instalovaný OS, IP adresa OS a přístupové údaje
- V případě hypervizoru, rozpis jednotlivých virtuálních serverů
- Virtuální serverová infrastruktura – popis každého serveru, jeho konfigurace po stránce HW tak SW a přístupové údaje
- Záruky na servery

Po dodání těchto informací musí dojít k fyzického kontrole uvedeného HW, a to jak po stránce vizuální, tak i přihlášením na tento HW.

Po uvedené analýze musí dojít k vytvoření nových administrátorských přístupů pro možnost správy HW a odebrání původních přístupů.

Následně budou převzaté systémy zaneseny do dokumentace, připraven návrh pravidelných zásahů na HW (update mikrokódů), zajištěno monitorování HW a nastavení SLA parametrů pro definovaný HW.

Během převzetí uvedené služby bude vypracována zpráva, ve které budou uvedeny zjištěné skutečnosti během přebíracího období a zároveň návrh činností pro zkvalitnění dodávané služby.

Po tomto kroku bude předložen akceptační protokol s uvedenými skutečnostmi z přebíracího období.

Následně dojde ke spuštění služby a zároveň k zahájení měření jednotlivých SLA parametrů, které budou pravidelně reportovány.

Přístup k řešení dané oblasti

Převzetí uvedené služby bude stanoveno dle standardních využívaných metodik a v závislosti na poskytovaných službách tak, aby nedošlo k omezení poskytovaných služeb a zároveň aby služba byla převzata s veškerými důležitými závislostmi na další poskytované služby a aby nedošlo k omezení těchto služeb během přebíracího období.

Oblast poskytování uvedené služby Správa serverové výpočetní infrastruktury HPe je závislé na Obecné pravidelné služby a SLA, Monitoring a dohledový systém, HelpDesk služby, Správa prostředí Managementu, SAN a diskových polí, Správa LAN prvků DC, Správa virtualizační platformy VMware, Správa služby MS Active Directory, Správa infrastrukturních služeb, Správa databázových serverů pro ORACLE, Správa databázových serverů pro MS SQL, Správa databázových serverů pro INFORMIX, Správa MS Windows serverů a Linux serverů.

V rámci přebíracího období musí být jasně specifikovány měřitelné parametry dle katalogového listu, pro zajištění vyhodnocování této služby. Jednotlivé parametry SLA budou vyhodnocovány z dohledového nástroje, který tyto parametry eviduje. Tyto měřitelné hodnoty bude obsahovat pravidelný report, ve kterém budou uvedené hodnoty a tím i informace o plnění uvedené služby.

Metodický a procesní postup převzetí služeb

Pro zajištění převzetí uvedené služby bude použita projektová metodika PRINCE2® dle které budou zajištěny veškeré náležitosti, jako jsou:

- Celkové naplánování převzetí služby – seznam dílčích kroků, jejich vzájemných vazeb a termínů zahájení a ukončení.
- Definice rizik v převzetí služby
- Koordinace třetích stran a optimalizovat potřebné součinnosti při převzetí služby.

Převzetí služby bude dále probíhat dle metodiky ITIL, která zajistí převzetí požadovaných služeb dle definovaných standardů. Použitá metodika bude řešit zejména níže uvedené oblasti.

- Definice požadované služby
- Nastavení služby
- Testovací provoz služby
- Validace služby
- Řízení změn
- Měření služby

Při převzetí služeb je nutné zohlednění metodik a politik v prostředí Zadavatele, a to zejména vydaných metodických pokynů a jednotlivých provozních řádů. Konkrétně se jedná o:

- Politika bezpečnosti informací Magistrátu hl. m. Prahy
- Technická bezpečnostní politika správy ICT
- Technická bezpečnostní politika sítí
- Technická bezpečnostní politika konfigurace ICT
- Instrukce pro přístup do oblastí zajištěných PZTS
- Metodický pokyn č. 7/2017–k řízení bezpečnostních událostí a bezpečnostních incidentů
- Metodický pokyn č. 8/2017 - Pravidla užívání informačního systému Magistrátu hl. m. Prahy
- Metodický pokyn č. 2/2018–k systému řízení IT služeb
- Metodický pokyn č. 1/2019 – Provozní řád datového centra DC4
- Metodický pokyn č. 2/2019 – Provozní řád datového centra DC5

Návrh harmonogramu

Detail činnosti	T+3	T+5	T+10	T+12	T+16	T+18	T+20
Příprava plánu převzetí							
Předání a seznámení se s dokumentací							
Provedení analýzy prostředí							
Ověření stavu záruk							

Kontrola jednotlivých prvků							
Nastavení oprávnění na prvky							
Nastavení návazných procesů - monitoring							
Workshop před převzetím služby							
Převzetí služby							

(T=počty dnů)

Požadovaná součinnost zadavatele

- Nastavení fyzického i elektronického přístupu k dotčeným systémům pro poskytovatele
- Dodání dokumentace prostředí IBM POWER a veškeré související infrastruktury, seznamu souvisejícího HW a SW
- Dodání souhrnu požadovaných provozních parametrů IBM POWER
- Detailní informace ke každému serveru
    - kompletní konfigurace všech součástí serverů
    - stavy záruk
    - Verze instalovaného operačního systému
    - Přístupové oprávnění na management těchto serverů
- Seznam aplikací, které jsou provozovány na serverech a seznam administrátorů zodpovědných za aplikace
- Nastavení kontaktních a zodpovědných osob do kontaktní matice, a to včetně kontaktů pro komunikaci s dalšími navazujícími službami
- Dodání přístupových oprávnění ke všem příslušným systémům
- Stanovení vzoru pravidelného reportingu
- Zajištění VPN připojení

Požadovaná součinnost by neměla přesáhnout pracnost 3 MD

Analýza rizik v dané oblasti

V rámci analýzy a řízení rizik je potřeba postupovat následujícími kroky „Identifikace" -> „Hodnocení" -> „Implementace". Analýza rizik je prováděna dle odhadnuté pravděpodobnosti a dopadu.

Pro převzetí uvedené služby jsme identifikovaly následující rizika:

Riziko	Hodnocení rizika	Návrh nápravného opatření
Nedodržení časového harmonogramu	Střední	Včasné zajištění veškerých potřebných podkladů a součinností pro převzetí služby
Nedostatečný přístup k informacím pro provedení analýzy	Střední	Včasné předání veškerých potřebných informací a přístupů pro provedení analýzy, správné nastavení komunikační matice
Nedostatečná nebo žádná dokumentace k systémům	Střední	Zajistit podporu objednatele, stanovení odpovědnosti na straně

		objednatele a zajištění potřebných vstupů. Detailní validace dokumentace vůči skutečnosti.
Poškození dat	Střední	Pro minimalizování rizika je nutné mít zajištěny zálohy dohledového systému
Nesoučinnost třetích stran	Střední	Včasné kontaktování třetích stran pro zajištění potřebných součinností, stanovení odpovědnosti a rozhodovací pravomoci na straně objednatele
Nezajištění fyzického nebo elektronického přístupu k systémům	Nízké	Včasné otevření komunikace o přístupech a všech nutných podmínkách
Nezajištění všech nutných přístupových oprávnění (účtů) k systémům	Nízké	Zajistit včasnou validaci všech účtů a oprávnění nutných pro provedení převzetí i následné poskytování služby
Nesprávné kontakty v komunikační matici	Nízké	Zajistit včasnou validaci všech kontaktů nutných pro provedení převzetí i následné poskytování služby
Chybějící návaznost na ostatní služby a chybějící kontakt pro případ potřeby.	Nízké	Ověřit všechny vazby ostatních služeb na infra SUN Sparc. Zajistit a validovat kontakty u všech navazujících služeb, které budou v případě potřeby spolupracovat
Systémy bez podpory	Vysoké	Zajištění základní servisní podpory provozovaných systémů
Nepodporované verze mikrokódů	Střední	Zajištění aktualizace verze mikrokódů na podporovanou verzi výrobce

KL05 – Správa prostředí Managementu, SAN a diskových polí

Popis návrhu převzetí služeb

Před převzetím služby je nutné nejdříve stanovit jasný plán převzetí. Tento plán musí obsahovat: Vymezení hlavních kontaktních osob, definice procesů, způsob omezování rizik, definice akceptačních kritérií a harmonogram převzetí služeb.

Následně bude nutné jasně specifikovat procesy v rámci převzetí služeb, a to zejména v oblasti kontroly změn, kontroly sporných skutečností a kontroly rizik v převzetí služby. Dále bude nutné vytvořit komunikační matici pro nastavení komunikačních kanálů v této oblasti pro zajištění informovanosti při přebíracím období. V rámci přebíracího období bude definován popis Implementačních kritérií, procesu testování a akceptace připravenosti na započetí poskytování Cílových služeb. Při převzetí služeb bude zohledněn dopady na zaměstnance koncového Zákazníka, dopad na interní procesy a postupy koncového Zákazníka, připravenost vybavení, rozhraní a procesů nutných pro bezproblémové zahájení poskytování Cílových služeb, finanční a obchodní dopady zahájení poskytování Cílových služeb.

V rámci převzetí této služby je nejprve nutné provést analýzu této oblasti. Je nutné zajistit detailní dokumentaci k danému prostředí, zejména je nutné zajistit kompletní seznam HW, který bude obsahovat detailní popis HW a komponent, jejich umístění, výrobní čísla machine type a serial number případně service tag HW, verze mikrokódů jednotlivých HW, stavy záruk jednotlivých zařízení, seznam administrátorských přístupů s IP adresami, seznam připojených serverů ke storage a seznam kontaktů zodpovědných za dané systémy. Nedílnou součástí této analýzy by mělo být dodání ze strany zadavatele vazby na jednotlivý HW z pohledu celé architektury prostředí.

Předpokladem je dokumentace, obsahující následující informace:

- Jednotlivé storage technologie jejich označení model/typ/sériové číslo
- HW konfigurace storage, počet kontrolerů, velikost cache, počet expanzí a disků
- Verze mikrokódů (FW) storage
- IP adresy managementu storage a přístupové údaje
- Soupis jednotlivých poolů, virtuálních disků
- Seznam připojených serverů
- Seznam mapovaných disků k jednotlivým serverům
- Záruky na storage

Samostatnou částí je SAN topologie. U SANu je potřeba mít zmapované propojení jednotlivých switchů, nastavení zónování switchů, tedy propojení mezi servery, storage, páskovou knihovnou.

- Jednotlivé SAN technologie jejich označení model/typ/sériové číslo
- SAN konfigurace, počet switchů, propojení (pokud je realizované)
- Verze mikrokódů (FW) SAN switchů
- IP adresy managementu SAN switchů a přístupové údaje
- Aktivní konfigurace (zoning) SAN switchů, seznam zapojených zařízení
- Schématické znázornění topologie SAN

Následně budou převzaté systémy zaneseny do dokumentace, připraven návrh pravidelných zásahů na HW (update mikrokódů), zajištěno monitorování HW a nastavení SLA parametrů pro definovaný HW.

Během převzetí uvedené služby bude vypracována zpráva, ve které budou uvedeny zjištěné skutečnosti během přebíracího období a zároveň návrh činností pro zkvalitnění dodávané služby.

Po tomto kroku bude předložen akceptační protokol s uvedenými skutečnostmi z přebíracího období.

Následně dojde ke spuštění služby a zároveň k zahájení měření jednotlivých SLA parametrů, které budou pravidelně reportovány.

Přístup k řešení dané oblasti

Převzetí uvedené služby bude stanoveno dle standardních využívaných metodik a v závislosti na poskytovaných službách tak, aby nedošlo k omezení poskytovaných služeb a zároveň aby služba byla převzata s veškerými důležitými závislostmi na další poskytované služby a aby nedošlo k omezení těchto služeb během přebíracího období.

Oblast poskytování uvedené služby Správa prostředí Managementu, SAN a diskových polí je je závislé na Obecné pravidelné služby a SLA, HelpDesk služby, Správa serverové výpočetní infrastruktury SUN Sparc, SUN Enterprise, Správa serverové výpočetní infrastruktury IBM x86, Správa serverové výpočetní infrastruktury IBM POWER, Správa serverové výpočetní infrastruktury HPe, Správa LAN prvků DC, Správa virtualizační platformy VMware, Správa služby MS Active Directory, Správa služby Certifikační autorita, Správa infrastrukturních služeb, Správa databázových serverů pro ORACLE, Správa databázových serverů pro MS SQL, Správa databázových serverů pro INFORMIX, Správa služby MS Exchange Server, Správa MS Windows serverů a Linux serverů.

V rámci přebíracího období musí být jasně specifikovány měřitelné parametry dle katalogového listu, pro zajištění vyhodnocování této služby. Jednotlivé parametry SLA budou vyhodnocovány z dohledového nástroje, který tyto parametry eviduje. Tyto měřitelné hodnoty bude obsahovat pravidelný report, ve kterém budou uvedené hodnoty a tím i informace o plnění uvedené služby.

Metodický a procesní postup převzetí služeb

Pro zajištění převzetí uvedené služby bude použita projektová metodika PRINCE2® dle které budou zajištěny veškeré náležitosti, jako jsou:

- Celkové naplánování převzetí služby – seznam dílčích kroků, jejich vzájemných vazeb a termínů zahájení a ukončení.
- Definice rizik v převzetí služby
- Koordinace třetích stran a optimalizovat potřebné součinnosti při převzetí služby.

Převzetí služby bude dále probíhat dle metodiky ITIL, která zajistí převzetí požadovaných služeb dle definovaných standardů. Použitá metodika bude řešit zejména níže uvedené oblasti.

- Definice požadované služby
- Nastavení služby
- Testovací provoz služby
- Validace služby

- Řízení změn
- Měření služby

Při převzetí služeb je nutné zohlednění metodik a politik v prostředí Zadavatele, a to zejména vydaných metodických pokynů a jednotlivých provozních řádů. Konkrétně se jedná o:

- Politika bezpečnosti informací Magistrátu hl. m. Prahy
- Technická bezpečnostní politika správy ICT
- Technická bezpečnostní politika sítí
- Technická bezpečnostní politika konfigurace ICT
- Instrukce pro přístup do oblastí zajištěných PZTS
- Metodický pokyn č. 7/2017–k řízení bezpečnostních událostí a bezpečnostních incidentů
- Metodický pokyn č. 8/2017 - Pravidla užívání informačního systému Magistrátu hl. m. Prahy
- Metodický pokyn č. 2/2018–k systému řízení IT služeb
- Metodický pokyn č. 1/2019 – Provozní řád datového centra DC4
- Metodický pokyn č. 2/2019 – Provozní řád datového centra DC5

Návrh harmonogramu

Detail činnosti	T+2	T+4	T+8	T+10	T+13	T+15	T+18
Příprava plánu převzetí							
Předání a seznámení se s dokumentací							
Provedení analýzy prostředí							
Ověření stavu záruk							
Kontrola jednotlivých prvků - zoning							
Nastavení oprávnění na prvky							
Nastavení návazných procesů - monitoring							
Workshop před převzetím služby							
Převzetí služby							

(T=počty dnů)

Požadovaná součinnost zadavatele

- Seznam diskových polí a jejich umístění
- Nastavení fyzického i elektronického přístupu k dotčeným systémům pro poskytovatele
- Dodání dokumentace managementu, SAN a diskových polí a veškeré související infrastruktury, seznamu souvisejícího HW a SW
- Dodání seznamu serverů a aplikací využívající diskové pole
- Dodání souhrnu požadovaných provozních parametrů managementu, SAN a diskových polí
- Dodání přístupových oprávnění ke všem příslušným systémům
- Stanovení vzoru pravidelného reportingu
- Zajištění VPN přístupu

Požadovaná součinnost by neměla přesáhnout pracnost 3 MD

Analýza rizik v dané oblasti

V rámci analýzy a řízení rizik je potřeba postupovat následujícími kroky „Identifikace" -> „Hodnocení" -> „Implementace". Analýza rizik je prováděna dle odhadnuté pravděpodobnosti a dopadu.

Pro převzetí uvedené služby jsme identifikovaly následující rizika:

Riziko	Hodnocení rizika	Návrh nápravného opatření
Nedodržení časového harmonogramu	Střední	Včasné zajištění veškerých potřebných podkladů a součinností pro převzetí služby
Nedostatečný přístup k informacím pro provedení analýzy	Střední	Včasné předání veškerých potřebných informací a přístupů pro provedení analýzy, správné nastavení komunikační matice
Nedostatečná nebo žádná dokumentace k systémům	Střední	Zajistit podporu objednatele, stanovení odpovědnosti na straně objednatele a zajištění potřebných vstupů. Detailní validace dokumentace vůči skutečnosti.
Nesoučinnost třetích stran	Střední	Včasné kontaktování třetích stran pro zajištění potřebných součinností, stanovení odpovědnosti a rozhodovací pravomoci na straně objednatele
Nezajištění fyzického nebo elektronického přístupu k systémům	Nízké	Včasné otevření komunikace o přístupech a všech nutných podmínkách
Nezajištění všech nutných přístupových oprávnění (účtů) k systémům	Nízké	Zajistit včasnou validaci všech účtů a oprávnění nutných pro provedení převzetí i následné poskytování služby
Nesprávné kontakty v komunikační matici	Nízké	Zajistit včasnou validaci všech kontaktů nutných pro provedení převzetí i následné poskytování služby
Chybějící návaznost na ostatní služby a chybějící kontakt pro případ potřeby.	Nízké	Ověřit všechny vazby ostatních služeb managementu, SAN a diskových polí

		Zajistit a validovat kontakty u všech navazujících služeb, které budou v případě potřeby spolupracovat
Poškození dat	Střední	Pro minimalizování rizika je nutné mít zajištěny zálohy dohledového systému
Systémy bez podpory	Vysoké	Zajištění základní servisní podpory provozovaných systémů
Nepodporované verze mikrokódů	Střední	Zajištění aktualizace verze mikrokódů na podporovanou verzi výrobce

KL06 – Správa LAN prvků DC

Popis návrhu převzetí služeb

Před převzetím služby je nutné nejdříve stanovit jasný plán převzetí. Tento plán musí obsahovat: Vymezení hlavních kontaktních osob, definice procesů, způsob omezování rizik, definice akceptačních kritérií a harmonogram převzetí služeb.

Následně bude nutné jasně specifikovat procesy v rámci převzetí služeb, a to zejména v oblasti kontroly změn, kontroly sporných skutečností a kontroly rizik v převzetí služby. Dále bude nutné vytvořit komunikační matici pro nastavení komunikačních kanálů v této oblasti pro zajištění informovanosti při přebíracím období. V rámci přebíracího období bude definován popis Implementačních kritérií, procesu testování a akceptace připravenosti na započetí poskytování Cílových služeb. Při převzetí služeb bude zohledněn dopady na zaměstnance koncového Zákazníka, dopad na interní procesy a postupy koncového Zákazníka, připravenost vybavení, rozhraní a procesů nutných pro bezproblémové zahájení poskytování Cílových služeb, finanční a obchodní dopady zahájení poskytování Cílových služeb.

V rámci převzetí této služby je nejprve nutné provést analýzu této oblasti. Je nutné zajistit detailní dokumentaci k danému prostředí, zejména je nutné zajistit kompletní seznam síťových prvků, který bude obsahovat detailní popis jednotlivých prvků, jejich umístění, výrobní čísla verze mikrokódů jednotlivých HW, stavy záruk jednotlivých zařízení a seznam administrátorských přístupů s IP adresami. Dále je nutné dodat kompletní adresní plán celého prostředí a nákres síťové topologie v prostředí.

Po dodání uvedených informací a podkladů je nutné zajistit přístup na uvedené prvky a provést fyzickou kontrolu nastavení síťových prvků a provést zálohu konfigurace aktuálního nastavení. Následně bude provedena kontrola virtualizovaného prostředí v závislosti na síťovém nastavení a bude provedena kontrola aktuálnosti instalovaných verzí mikrokódů.

Následně budou převzaté systémy zaneseny do dokumentace, připraven návrh pravidelných zásahů na HW (update mikrokódů), zajištěno monitorování HW a nastavení SLA parametrů pro definovaný HW.

Během převzetí uvedené služby bude vypracována zpráva, ve které budou uvedeny zjištěné skutečnosti během přebíracího období a zároveň návrh činností pro zkvalitnění dodávané služby.

Po tomto kroku bude předložen akceptační protokol s uvedenými skutečnostmi z přebíracího období.

Následně dojde ke spuštění služby a zároveň k zahájení měření jednotlivých SLA parametrů, které budou pravidelně reportovány.

Přístup k řešení dané oblasti

Převzetí uvedené služby bude stanoveno dle standardních využívaných metodik a v závislosti na poskytovaných službách tak, aby nedošlo k omezení poskytovaných služeb a zároveň aby služba byla převzata s veškerými důležitými závislostmi na další poskytované služby a aby nedošlo k omezení těchto služeb během přebíracího období.

Oblast poskytování uvedené služby Správa LAN prvků DC je závislé na Obecné pravidelné služby a SLA, Monitoring a dohledové služby, HelpDesk služby, Správa serverové výpočetní infrastruktury SUN Sparc, SUN Enterprise, Správa serverové výpočetní infrastruktury IBM x86, Správa serverové výpočetní infrastruktury IBM POWER, Správa serverové výpočetní infrastruktury HPe, Správa prostředí Managementu, SAN a diskových polí, Správa virtualizační platformy VMware, Správa služby MS Active Directory, Správa služby Certifikační autorita, Správa infrastrukturních služeb, Správa databázových serverů pro ORACLE, Správa databázových serverů pro MS SQL, Správa databázových serverů pro INFORMIX, Správa služby MS Exchange Server, Správa MS Windows serverů a Linux serverů.

V rámci přebíracího období musí být jasně specifikovány měřitelné parametry dle katalogového listu, pro zajištění vyhodnocování této služby. Jednotlivé parametry SLA budou vyhodnocovány z dohledového nástroje, který tyto parametry eviduje. Tyto měřitelné hodnoty bude obsahovat pravidelný report, ve kterém budou uvedené hodnoty a tím i informace o plnění uvedené služby.

Metodický a procesní postup převzetí služeb

Pro zajištění převzetí uvedené služby bude použita projektová metodika PRINCE2® dle které budou zajištěny veškeré náležitosti, jako jsou:

- Celkové naplánování převzetí služby – seznam dílčích kroků, jejich vzájemných vazeb a termínů zahájení a ukončení
- Definice rizik v převzetí služby
- Koordinace třetích stran a optimalizovat potřebné součinnosti při převzetí služby

Převzetí služby bude dále probíhat dle metodiky ITIL, která zajistí převzetí požadovaných služeb dle definovaných standardů. Použitá metodika bude řešit zejména níže uvedené oblasti.

- Definice požadované služby
- Nastavení služby
- Testovací provoz služby
- Validace služby

- Řízení změn
- Měření služby

Při převzetí služeb je nutné zohlednění metodik a politik v prostředí Zadavatele, a to zejména vydaných metodických pokynů a jednotlivých provozních řádů. Konkrétně se jedná o:

- Politika bezpečnosti informací Magistrátu hl. m. Prahy
- Technická bezpečnostní politika správy ICT
- Technická bezpečnostní politika sítí
- Technická bezpečnostní politika konfigurace ICT
- Instrukce pro přístup do oblastí zajištěných PZTS
- Metodický pokyn č. 7/2017–k řízení bezpečnostních událostí a bezpečnostních incidentů
- Metodický pokyn č. 8/2017 - Pravidla užívání informačního systému Magistrátu hl. m. Prahy
- Metodický pokyn č. 2/2018–k systému řízení IT služeb
- Metodický pokyn č. 1/2019 – Provozní řád datového centra DC4
- Metodický pokyn č. 2/2019 – Provozní řád datového centra DC5

Návrh harmonogramu

Detail činnosti	T+2	T+4	T+10	T+12	T+14	T+16	T+18
Příprava plánu převzetí							
Předání a seznámení se s dokumentací							
Provedení analýzy prostředí							
Ověření stavu záruk							
Kontrola jednotlivých prvků							
Nastavení oprávnění na prvky							
Nastavení návazných procesů - monitoring							
Workshop před převzetím služby							
Převzetí služby							

(T=počty dnů)

Požadovaná součinnost zadavatele

- Dodání seznamu prvků (SN, IP adresy, umístění, verze operačního systému, stavy záruk)
- Dodání adresního plánu
- Dodání nákresu síťové topologie
- Nastavení fyzického i elektronického přístupu k dotčeným systémům pro poskytovatele
- Dodání dokumentace infrastruktury a veškeré související infrastruktury, seznamu souvisejícího HW a SW, seznamu a obsahu procesů
- Přístupy do supportních portálů
- Dodání přístupových oprávnění ke všem příslušným systémům
- Nastavení kontaktních a zodpovědných osob do kontaktní matice, a to včetně kontaktů pro komunikaci s dalšími navazujícími službami
- Stanovení vzoru pravidelného reportingu

- Zajištění VPN přístupu

Požadovaná součinnost by neměla přesáhnout pracnost 3 MD

Analýza rizik v dané oblasti

V rámci analýzy a řízení rizik je potřeba postupovat následujícími kroky „Identifikace" -> „Hodnocení" -> „Implementace". Analýza rizik je prováděna dle odhadnuté pravděpodobnosti a dopadu.

Pro převzetí uvedené služby jsme identifikovaly následující rizika:

Riziko	Hodnocení rizika	Návrh nápravného opatření
Nedodržení časového harmonogramu	Střední	Včasné zajištění veškerých potřebných podkladů a součinností pro převzetí služby
Nedostatečný přístup k informacím pro provedení analýzy	Střední	Včasné předání veškerých potřebných informací a přístupů pro provedení analýzy, správné nastavení komunikační matice
Nedostatečná nebo žádná dokumentace k systémům	Střední	Zajistit podporu objednatele, stanovení odpovědnosti na straně objednatele a zajištění potřebných vstupů. Detailní validace dokumentace vůči skutečnosti.
Nesoučinnost třetích stran	Střední	Včasné kontaktování třetích stran pro zajištění potřebných součinností, stanovení odpovědnosti a rozhodovací pravomoci na straně objednatele
Nezajištění fyzického nebo elektronického přístupu k systémům	Nízké	Včasné otevření komunikace o přístupech a všech nutných podmínkách
Nezajištění všech nutných přístupových oprávnění (účtů) k systémům	Nízké	Zajistit včasnou validaci všech účtů a oprávnění nutných pro provedení převzetí i následné poskytování služby
Nesprávné kontakty v komunikační matici	Nízké	Zajistit včasnou validaci všech kontaktů nutných pro provedení převzetí i následné poskytování služby
Chybějící návaznost na ostatní služby a chybějící	Nízké	Ověřit všechny vazby ostatních služeb na

kontakt pro případ potřeby.		virtualizační infrastruktury. Zajistit a validovat kontakty u všech navazujících služeb, které budou v případě potřeby spolupracovat
Systémy bez podpory	Střední	Zajištění základní servisní podpory provozovaných systémů
Nekompletní adresní plán	Střední	Včasné zajištění a kompletace adresního plánu v prostředí

KL07 – Správa virtualizační platformy VMware

Popis návrhu převzetí služeb

Před převzetím služby je nutné nejdříve stanovit jasný plán převzetí. Tento plán musí obsahovat: Vymezení hlavních kontaktních osob, definice procesů, způsob omezování rizik, definice akceptačních kritérií a harmonogram převzetí služeb.

Následně bude nutné jasně specifikovat procesy v rámci převzetí služeb, a to zejména v oblasti kontroly změn, kontroly sporných skutečností a kontroly rizik v převzetí služby. Dále bude nutné vytvořit komunikační matici pro nastavení komunikačních kanálů v této oblasti pro zajištění informovanosti při přebíracím období. V rámci přebíracího období bude definován popis Implementačních kritérií, procesu testování a akceptace připravenosti na započetí poskytování Cílových služeb. Při převzetí služeb bude zohledněn dopady na zaměstnance koncového Zákazníka, dopad na interní procesy a postupy koncového Zákazníka, připravenost vybavení, rozhraní a procesů nutných pro bezproblémové zahájení poskytování Cílových služeb, finanční a obchodní dopady zahájení poskytování Cílových služeb.

Před převzetím této služby je nejprve nutné provést analýzu této oblasti. Je nutné zajistit detailní dokumentaci k danému prostředí, které musí obsahovat veškeré náležitosti, dále je nutné zajistit informace o použitých licencí. Je nutné provést kontrolu jednotlivých fyzických serverů kde je virtualizace využívána, prověřit verze jednotlivých ESX serverů a vCenter samotných a využívané služby ze strany virtualizace. Další důležitý bod celé architektura prostředí.

Po dodání těchto informací musí dojít k fyzického kontrole uvedeného HW/SW, a to jak po stránce vizuální, tak i fyzickým přihlášením na tento HW/SW.

Po uvedené analýze musí dojít k vytvoření nových administrátorských přístupů pro možnost správy prostředí a odebrání původních přístupů.

Následně budou převzaté systémy zaneseny do dokumentace, připraven návrh pravidelných zásahů na prostředí, zajištěno monitorování prostředí a nastavení SLA parametrů pro definované služby.

Po těchto krocích dojde k převzetí uvedené služby.

Přístup k řešení dané oblasti

Převzetí uvedené služby bude stanoveno dle standardních využívaných metodik a v závislosti na poskytovaných službách tak, aby nedošlo k omezení poskytovaných služeb a zároveň aby služba byla převzata s veškerými důležitými závislostmi na další poskytované služby a aby nedošlo k omezení těchto služeb během přebíracího období.

Oblast poskytování uvedené služby Správa virtualizační platformy VMware je je závislé na Obecné pravidelné služby a SLA, HelpDesk služby, Správa serverové výpočetní infrastruktury SUN Sparc, SUN Enterprise, Správa serverové výpočetní infrastruktury IBM x86, Správa serverové výpočetní infrastruktury IBM POWER, Správa serverové výpočetní infrastruktury HPe, Správa prostředí Managementu, SAN a diskových polí, Správa LAN prvků DC, Správa služby MS Active Directory, Správa služby Certifikační autorita, Správa infrastrukturních služeb, Správa databázových serverů pro ORACLE, Správa databázových serverů pro MS SQL, Správa databázových serverů pro INFORMIX, Správa služby MS Exchange Server, Správa MS Windows serverů a Linux serverů.

V rámci přebíracího období musí být jasně specifikovány měřitelné parametry dle katalogového listu, pro zajištění vyhodnocování této služby. Jednotlivé parametry SLA budou vyhodnocovány z dohledového nástroje, který tyto parametry eviduje. Tyto měřitelné hodnoty bude obsahovat pravidelný report, ve kterém budou uvedené hodnoty a tím i informace o plnění uvedené služby.

Metodický a procesní postup převzetí služeb

Pro zajištění převzetí uvedené služby bude použita projektová metodika PRINCE2® dle které budou zajištěny veškeré náležitosti, jako jsou:

- Celkové naplánování převzetí služby – seznam dílčích kroků, jejich vzájemných vazeb a termínů zahájení a ukončení.
- Definice rizik v převzetí služby
- Koordinace třetích stran a optimalizovat potřebné součinnosti při převzetí služby.

Převzetí služby bude dále probíhat dle metodiky ITIL, která zajistí převzetí požadovaných služeb dle definovaných standardů. Použitá metodika bude řešit zejména níže uvedené oblasti.

- Definice požadované služby
- Nastavení služby
- Testovací provoz služby
- Validace služby
- Řízení změn
- Měření služby

Při převzetí služeb je nutné zohlednění metodik a politik v prostředí Zadavatele, a to zejména vydaných metodických pokynů a jednotlivých provozních řádů. Konkrétně se jedná o:

- Politika bezpečnosti informací Magistrátu hl. m. Prahy
- Technická bezpečnostní politika správy ICT
- Technická bezpečnostní politika sítí

- Technická bezpečnostní politika konfigurace ICT
- Instrukce pro přístup do oblastí zajištěných PZTS
- Metodický pokyn č. 7/2017–k řízení bezpečnostních událostí a bezpečnostních incidentů
- Metodický pokyn č. 8/2017 - Pravidla užívání informačního systému Magistrátu hl. m. Prahy
- Metodický pokyn č. 2/2018–k systému řízení IT služeb
- Metodický pokyn č. 1/2019 – Provozní řád datového centra DC4
- Metodický pokyn č. 2/2019 – Provozní řád datového centra DC5

Návrh harmonogramu

Detail činnosti	T+2	T+4	T+6	T+10	T+12	T+15
Příprava plánu převzetí						
Předání a seznámení se s dokumentací						
Nastavení oprávnění						
Provedení analýzy prostředí						
Kontrola virtualizovaného prostředí						
Ověření licencí						
Nastavení návazných procesů - monitoring						
Workshop před převzetím služby						
Převzetí služby						

(T=počty dnů)

Požadovaná součinnost zadavatele

- Dodání seznamu fyzických serverů využívajících VMware
- Dokumentace prostředí VMware a použitých technologií
- Dodání informací k licencování prostředí
- Předání přístupu do licenčního portálu
- Zajištění přístupu do prostředí VMware
- Dodání souhrnu požadovaných provozních parametrů virtualizační infrastruktury
- Nastavení kontaktních a zodpovědných osob do kontaktní matice, a to včetně kontaktů pro komunikaci s dalšími navazujícími službami
- Zajištění VPN přístupu

Požadovaná součinnost by neměla přesáhnout pracnost 2 MD

Analýza rizik v dané oblasti

V rámci analýzy a řízení rizik je potřeba postupovat následujícími kroky „Identifikace" -> „Hodnocení" -> „Implementace". Analýza rizik je prováděna dle odhadnuté pravděpodobnosti a dopadu.

Pro převzetí uvedené služby jsme identifikovaly následující rizika:

Riziko	Hodnocení rizika	Návrh nápravného opatření
Nedodržení časového harmonogramu	Střední	Včasné zajištění veškerých potřebných podkladů a součinností pro převzetí

		služby
Nedostatečný přístup k informacím pro provedení analýzy	Střední	Včasné předání veškerých potřebných informací a přístupů pro provedení analýzy, správné nastavení komunikační matice
Nedostatečná nebo žádná dokumentace k provozovaným systémům	Střední	Zajistit podporu Zadavatele pro optimalizaci, stanovení odpovědnosti na straně Zadavatele a zajištění potřebných vstupů
Poškození dat	Střední	Pro minimalizování rizika je nutné mít zajištěny zálohy dohledového systému
Nesoučinnost třetích stran	Střední	Včasné kontaktování třetích stran pro zajištění potřebných součinností
Nedostatečné informace o řešení virtualizační infrastruktury	Nízké	Zajistit podporu objednatele, stanovení odpovědnosti na straně objednatele
Nezajištění fyzického nebo elektronického přístupu k systémům	Nízké	Včasné otevření komunikace o přístupech a všech nutných podmínkách
Nezajištění všech nutných přístupových oprávnění (účtů) k systémům	Nízké	Zajistit včasnou validaci všech účtů a oprávnění nutných pro provedení převzetí i následné poskytování služby
Nesprávné kontakty v komunikační matici	Nízké	Zajistit včasnou validaci všech kontaktů nutných pro provedení převzetí i následné poskytování služby
Chybějící návaznost na ostatní služby a chybějící kontakt pro případ potřeby.	Nízké	Ověřit všechny vazby ostatních služeb na virtualizační infrastruktury. Zajistit a validovat kontakty u všech navazujících služeb, které budou v případě potřeby spolupracovat
Systémy bez podpory	Vysoké	Zajištění základní servisní podpory provozovaných systémů

KL08 – Správa služby MS Active Directory

Popis návrhu převzetí služeb

Před převzetím služby je nutné nejdříve stanovit jasný plán převzetí. Tento plán musí obsahovat: Vymezení hlavních kontaktních osob, definice procesů, způsob omezování rizik, definice akceptačních kritérií a harmonogram převzetí služeb.

Následně bude nutné jasně specifikovat procesy v rámci převzetí služeb, a to zejména v oblasti kontroly změn, kontroly sporných skutečností a kontroly rizik v převzetí služby. Dále bude nutné vytvořit komunikační matici pro nastavení komunikačních kanálů v této oblasti pro zajištění informovanosti při přebíracím období. V rámci přebíracího období bude definován popis Implementačních kritérií, procesu testování a akceptace připravenosti na započetí poskytování Cílových služeb. Při převzetí služeb bude zohledněn dopady na zaměstnance koncového Zákazníka, dopad na interní procesy a postupy koncového Zákazníka, připravenost vybavení, rozhraní a procesů nutných pro bezproblémové zahájení poskytování cílových služeb, finanční a obchodní dopady zahájení poskytování cílových služeb.

V rámci převzetí musí dojít k převzetí přístupových oprávnění a servisních účtů. Následně musí být ověřen stav jednotlivých doménových kontrolerů a jejich služeb a vzájemné replikace. Je nutné prověřit jednotlivé stavy služeb a musí být prověřen procesy jednotlivých úkonů jako je tvorba účtů, přidělení oprávnění a podobně. Je taky nutné prověřit návaznosti na další aplikace jako je IDM a prověřit procesy spojené s centrálně řízenou identitou.

Následně budou převzaté systémy zaneseny do dokumentace, zajištěno monitorování uvedených systémů a nastavení SLA parametrů pro definované služby.

Během převzetí uvedené služby bude vypracována zpráva, ve které budou uvedeny zjištěné skutečnosti během přebíracího období a zároveň návrh činností pro zkvalitnění dodávané služby.

Po tomto kroku bude předložen akceptační protokol s uvedenými skutečnostmi z přebíracího období.

Následně dojde ke spuštění služby a zároveň k zahájení měření jednotlivých SLA parametrů, které budou pravidelně reportovány.

Přístup k řešení dané oblasti

Převzetí uvedené služby bude stanoveno dle standardních využívaných metodik a v závislosti na poskytovaných službách tak, aby nedošlo k omezení poskytovaných služeb a zároveň aby služba byla převzata s veškerými důležitými závislostmi na další poskytované služby a aby nedošlo k omezení těchto služeb během přebíracího období.

Oblast poskytování uvedené služby Správa služby Active Directory je závislé na Obecné pravidelné služby a SLA, Monitoring a dohledové systémy, HelpDesk služby, Správa serverové výpočetní infrastruktury SUN Sparc, SUN Enterprise, Správa serverové výpočetní infrastruktury IBM x86, Správa serverové výpočetní infrastruktury IBM POWER, Správa serverové výpočetní infrastruktury HPe, Správa prostředí Managementu, SAN a diskových

polí, Správa LAN prvků DC, Správa virtualizační platformy VMware, Správa služby Certifikační autorita, Správa infrastrukturních služeb, Správa databázových serverů pro ORACLE, Správa databázových serverů pro MS SQL, Správa databázových serverů pro INFORMIX, Správa služby MS Exchange Server, Správa MS Windows serverů a Linux serverů.

V rámci přebíracího období musí být jasně specifikovány měřitelné parametry dle katalogového listu, pro zajištění vyhodnocování této služby. Jednotlivé parametry SLA budou vyhodnocovány z dohledového nástroje, který tyto parametry eviduje. Tyto měřitelné hodnoty bude obsahovat pravidelný report, ve kterém budou uvedené hodnoty a tím i informace o plnění uvedené služby.

Metodický a procesní postup převzetí služeb

Pro zajištění převzetí uvedené služby bude použita projektová metodika PRINCE2® dle které budou zajištěny veškeré náležitosti, jako jsou:

- Celkové naplánování převzetí služby – seznam dílčích kroků, jejich vzájemných vazeb a termínů zahájení a ukončení.
- Definice rizik v převzetí služby
- Koordinace třetích stran a optimalizovat potřebné součinnosti při převzetí služby.

Převzetí služby bude dále probíhat dle metodiky ITIL, která zajistí převzetí požadovaných služeb dle definovaných standardů. Použitá metodika bude řešit zejména níže uvedené oblasti.

- Definice požadované služby
- Nastavení služby
- Testovací provoz služby
- Validace služby
- Řízení změn
- Měření služby

Při převzetí služeb je nutné zohlednění metodik a politik v prostředí Zadavatele, a to zejména vydaných metodických pokynů a jednotlivých provozních řádů. Konkrétně se jedná o:

- Politika bezpečnosti informací Magistrátu hl. m. Prahy
- Technická bezpečnostní politika správy ICT
- Technická bezpečnostní politika sítí
- Technická bezpečnostní politika konfigurace ICT
- Instrukce pro přístup do oblastí zajištěných PZTS
- Metodický pokyn č. 7/2017–k řízení bezpečnostních událostí a bezpečnostních incidentů
- Metodický pokyn č. 8/2017 - Pravidla užívání informačního systému Magistrátu hl. m. Prahy
- Metodický pokyn č. 2/2018–k systému řízení IT služeb
- Metodický pokyn č. 1/2019 – Provozní řád datového centra DC4
- Metodický pokyn č. 2/2019 – Provozní řád datového centra DC5

Návrh harmonogramu

Detail činnosti	T+2	T+4	T+6	T+8	T+10	T+14
Příprava plánu převzetí						
Předání a seznámení se s dokumentací						
Nastavení oprávnění						
Provedení analýzy prostředí						
Kontrola prostředí AD						
Nastavení návazných procesů - monitoring						
Workshop před převzetím služby						
Převzetí služby						

(T=počty dnů)

Požadovaná součinnost zadavatele

- Nastavení fyzického i elektronického přístupu k dotčeným systémům pro poskytovatele
- Dodání dokumentace AD a veškeré související infrastruktury, seznamu souvisejícího HW a SW, seznamu a obsahu procesů.
- Nastavení kontaktních a zodpovědných osob do kontaktní matice, a to včetně kontaktů pro komunikaci s dalšími navazujícími službami.
- Stanovení vzoru pravidelného reportingu
- Seznam doménových politik
- Zajištění VPN přístupu

Analýza rizik v dané oblasti

V rámci analýzy a řízení rizik je potřeba postupovat následujícími kroky „Identifikace" -> „Hodnocení" -> „Implementace". Analýza rizik je prováděna dle odhadnuté pravděpodobnosti a dopadu.

Pro převzetí uvedené služby jsme identifikovaly následující rizika:

Riziko	Hodnocení rizika	Návrh nápravného opatření
Nedodržení časového harmonogramu	Střední	Včasné zajištění veškerých potřebných podkladů a součinností pro převzetí služby
Nedostatečný přístup k informacím pro provedení analýzy	Střední	Včasné předání veškerých potřebných informací a přístupů pro provedení analýzy, správné nastavení komunikační matice
Nedostatečná nebo žádná dokumentace k systémům,	Střední	Zajistit podporu objednatele, stanovení

případně rozpory mezi dokumentací a skutečným stavem		odpovědnosti na straně objednatele a zajištění potřebných vstupů. Detailní validace dokumentace vůči skutečnosti a případná oprava dokumentace dle stavu.
Nesoučinnost třetích stran	Střední	Včasné kontaktování třetích stran pro zajištění potřebných součinností, stanovení odpovědnosti a rozhodovací pravomoci na straně objednatele
Nezajištění fyzického nebo elektronického přístupu k systémům	Nízké	Včasné otevření komunikace o přístupech a všech nutných podmínkách
Nezajištění všech nutných přístupových oprávnění (účtů) k systémům	Nízké	Zajistit včasnou validaci všech účtů a oprávnění nutných pro provedení převzetí i následné poskytování služby
Nesprávné kontakty v komunikační matici	Nízké	Zajistit včasnou validaci všech kontaktů nutných pro provedení převzetí i následné poskytování služby
Poškození dat	Střední	Pro minimalizování rizika je nutné mít zajištěny zálohy dohledového systému
Systémy bez podpory	Střední	Zajištění základní servisní podpory provozovaných systémů

KL09 – Správa služby Certifikační autorita

Popis návrhu převzetí služeb

Před převzetím služby je nutné nejdříve stanovit jasný plán převzetí. Tento plán musí obsahovat: Vymezení hlavních kontaktních osob, definice procesů, způsob omezování rizik, definice akceptačních kritérií a harmonogram převzetí služeb.

Následně bude nutné jasně specifikovat procesy v rámci převzetí služeb, a to zejména v oblasti kontroly změn, kontroly sporných skutečností a kontroly rizik v převzetí služby. Dále bude nutné vytvořit komunikační matici pro nastavení komunikačních kanálů v této oblasti pro zajištění informovanosti při přebíracím období. V rámci přebíracího období bude definován popis Implementačních kritérií, procesu testování a akceptace připravenosti na započetí poskytování Cílových služeb. Při převzetí služeb bude zohledněn dopady na

zaměstnance koncového Zákazníka, dopad na interní procesy a postupy koncového Zákazníka, připravenost vybavení, rozhraní a procesů nutných pro bezproblémové zahájení poskytování Cílových služeb, finanční a obchodní dopady zahájení poskytování Cílových služeb.

V rámci převzetí této služby je nutné zkontrolovat dokumentaci prostředí certifikační autority a stav serverů certifikační autority. Dále je nutné zajistit zejména předání servisních účtů a hesel k root certifikátům. Následně musí dojít k přihlášení na servery CA a provedení faktické kontroly. Musí být zkontrolovány pravidelné činnosti spojené k SubCA a rootCA.

Následně budou převzaté systémy zaneseny do dokumentace, zajištěno monitorování uvedených systémů a nastavení SLA parametrů pro definované služby.

Během převzetí uvedené služby bude vypracována zpráva, ve které budou uvedeny zjištěné skutečnosti během přebíracího období a zároveň návrh činností pro zkvalitnění dodávané služby.

Po tomto kroku bude předložen akceptační protokol s uvedenými skutečnostmi z přebíracího období.

Následně dojde ke spuštění služby a zároveň k zahájení měření jednotlivých SLA parametrů, které budou pravidelně reportovány.

Přístup k řešení dané oblasti

Převzetí uvedené služby bude stanoveno dle standardních využívaných metodik a v závislosti na poskytovaných službách tak, aby nedošlo k omezení poskytovaných služeb a zároveň aby služba byla převzata s veškerými důležitými závislostmi na další poskytované služby a aby nedošlo k omezení těchto služeb během přebíracího období.

Oblast poskytování uvedené služby Správa certifikační autority je závislé na Obecné pravidelné služby a SLA, Monitoring a dohledové systémy, HelpDesk služby, Správa serverové výpočetní infrastruktury SUN Sparc, SUN Enterprise, Správa serverové výpočetní infrastruktury IBM x86, Správa serverové výpočetní infrastruktury IBM POWER, Správa serverové výpočetní infrastruktury HPe, Správa prostředí Managementu, SAN a diskových polí, Správa LAN prvků DC, Správa virtualizační platformy VMware, Správa služby MS Active Directory, Správa infrastrukturních služeb, Správa databázových serverů pro ORACLE, Správa databázových serverů pro MS SQL, Správa databázových serverů pro INFORMIX, Správa služby MS Exchange Server, Správa MS Windows serverů a Linux serverů.

V rámci přebíracího období musí být jasně specifikovány měřitelné parametry dle katalogového listu, pro zajištění vyhodnocování této služby. Jednotlivé parametry SLA budou vyhodnocovány z dohledového nástroje, který tyto parametry eviduje. Tyto měřitelné hodnoty bude obsahovat pravidelný report, ve kterém budou uvedené hodnoty a tím i informace o plnění uvedené služby.

Metodický a procesní postup převzetí služeb

Pro zajištění převzetí uvedené služby bude použita projektová metodika PRINCE2® dle které budou zajištěny veškeré náležitosti, jako jsou:

- Celkové naplánování převzetí služby – seznam dílčích kroků, jejich vzájemných vazeb a termínů zahájení a ukončení
- Definice rizik v převzetí služby
- Koordinace třetích stran a optimalizovat potřebné součinnosti při převzetí služby

Převzetí služby bude dále probíhat dle metodiky ITIL, která zajistí převzetí požadovaných služeb dle definovaných standardů. Použitá metodika bude řešit zejména níže uvedené oblasti.

- Definice požadované služby
- Nastavení služby
- Testovací provoz služby
- Validace služby
- Řízení změn
- Měření služby

Při převzetí služeb je nutné zohlednění metodik a politik v prostředí Zadavatele, a to zejména vydaných metodických pokynů a jednotlivých provozních řádů. Konkrétně se jedná o:

- Politika bezpečnosti informací Magistrátu hl. m. Prahy
- Technická bezpečnostní politika správy ICT
- Technická bezpečnostní politika sítí
- Technická bezpečnostní politika konfigurace ICT
- Instrukce pro přístup do oblastí zajištěných PZTS
- Metodický pokyn č. 7/2017–k řízení bezpečnostních událostí a bezpečnostních incidentů
- Metodický pokyn č. 8/2017 - Pravidla užívání informačního systému Magistrátu hl. m. Prahy
- Metodický pokyn č. 2/2018–k systému řízení IT služeb
- Metodický pokyn č. 1/2019 – Provozní řád datového centra DC4
- Metodický pokyn č. 2/2019 – Provozní řád datového centra DC5

Návrh harmonogramu

Detail činnosti	T+2	T+3	T+6	T+8	T+10	T+12
Příprava plánu převzetí						
Předání a seznámení se s dokumentací						
Nastavení oprávnění						
Provedení analýzy prostředí						
Kontrola prostředí CA						
Ověření přidělených certifikátů						
Nastavení návazných procesů - monitoring						
Workshop před převzetím služby						
Převzetí služby						

(T=počty dnů)

Požadovaná součinnost zadavatele

- Nastavení fyzického i elektronického přístupu k dotčeným systémům pro poskytovatele
- Dodání dokumentace Certifikační Autority
- Zřízení přístupů, nastavení oprávnění
- Nastavení kontaktních a zodpovědných osob do kontaktní matice, a to včetně kontaktů pro komunikaci s dalšími navazujícími službami
- Stanovení vzoru pravidelného reportingu
- Zajištění VPN přístupu

Analýza rizik v dané oblasti

V rámci analýzy a řízení rizik je potřeba postupovat následujícími kroky „Identifikace" -> „Hodnocení" -> „Implementace". Analýza rizik je prováděna dle odhadnuté pravděpodobnosti a dopadu.

Pro převzetí uvedené služby jsme identifikovaly následující rizika:

Riziko	Hodnocení rizika	Návrh nápravného opatření
Nedodržení časového harmonogramu	Střední	Včasné zajištění veškerých potřebných podkladů a součinností pro převzetí služby
Nedostatečný přístup k informacím pro provedení analýzy	Střední	Včasné předání veškerých potřebných informací a přístupů pro provedení analýzy, správné nastavení komunikační matice
Nedostatečná nebo žádná dokumentace k systémům, případně rozpory mezi dokumentací a skutečným stavem	Střední	Zajistit podporu objednatele, stanovení odpovědnosti na straně objednatele a zajištění potřebných vstupů. Detailní validace dokumentace vůči skutečnosti a případná oprava dokumentace dle stavu.
Poškození dat	Střední	Pro minimalizování rizika je nutné mít zajištěny zálohy dohledového systému
Nesoučinnost třetích stran	Střední	Včasné kontaktování třetích stran pro zajištění potřebných součinností, stanovení odpovědnosti a rozhodovací pravomoci na straně objednatele

Nezajištění fyzického nebo elektronického přístupu k systémům	Nízké	Včasné otevření komunikace o přístupech a všech nutných podmínkách
Nezajištění všech nutných přístupových oprávnění (účtů) k systémům	Nízké	Zajistit včasnou validaci všech účtů a oprávnění nutných pro provedení převzetí i následné poskytování služby
Nesprávné kontakty v komunikační matici	Nízké	Zajistit včasnou validaci všech kontaktů nutných pro provedení převzetí i následné poskytování služby
Systémy bez podpory	Střední	Zajištění základní servisní podpory provozovaných systémů

KL10 – Správa infrastrukturních služeb

Popis návrhu převzetí služeb

Před převzetím služby je nutné nejdříve stanovit jasný plán převzetí. Tento plán musí obsahovat: Vymezení hlavních kontaktních osob, definice procesů, způsob omezování rizik, definice akceptačních kritérií a harmonogram převzetí služeb.

Následně bude nutné jasně specifikovat procesy v rámci převzetí služeb, a to zejména v oblasti kontroly změn, kontroly sporných skutečností a kontroly rizik v převzetí služby. Dále bude nutné vytvořit komunikační matici pro nastavení komunikačních kanálů v této oblasti pro zajištění informovanosti při přebíracím období. V rámci přebíracího období bude definován popis Implementačních kritérií, procesu testování a akceptace připravenosti na započetí poskytování Cílových služeb. Při převzetí služeb bude zohledněn dopady na zaměstnance koncového Zákazníka, dopad na interní procesy a postupy koncového Zákazníka, připravenost vybavení, rozhraní a procesů nutných pro bezproblémové zahájení poskytování Cílových služeb, finanční a obchodní dopady zahájení poskytování Cílových služeb.

Před převzetím této služby je nejprve nutné provést analýzu této oblasti. Je nutné zajistit detailní dokumentaci k danému prostředí, které musí obsahovat veškeré náležitosti k jednotlivým technologiím. Zejména pak pravidla, kterými se uvedené systémy řídí.

U systému DNS je nutné jasné specifikace nastavení lokalit versus konkrétní servery, jmenná konvence, omezení přístupu do DNS systému, seznam domén, které mají být v rámci katalogové listu spravovány a také informace o interních a externích DNS zónách.

Pro systém NTP je nutné dodat seznam všech NTP serverů v prostředí zadavatele a jejich popis nastavení.

U systému DHCP je nutné specifikovat jasný adresní IP plán ve vztahu celého prostředí a jeho segmentace, pravidla pro řízení uvedené služby a celkově nastavená politika řízení této služby. Musí také dojít ke kontrole jednotlivých DHCP serverů.

Pro systém TACACS RADIUS je nutné specifikovat pravidla za kterých je možno provádět změny a hlavně jaké služby systém využívají a jak.

Následně budou převzaté systémy zaneseny do dokumentace, zajištěno monitorování uvedených systémů a nastavení SLA parametrů pro definované služby.

Během převzetí uvedené služby bude vypracována zpráva, ve které budou uvedeny zjištěné skutečnosti během přebíracího období a zároveň návrh činností pro zkvalitnění dodávané služby.

Po tomto kroku bude předložen akceptační protokol s uvedenými skutečnostmi z přebíracího období.

Následně dojde ke spuštění služby a zároveň k zahájení měření jednotlivých SLA parametrů, které budou pravidelně reportovány.

Přístup k řešení dané oblasti

Převzetí uvedené služby bude stanoveno dle standardních využívaných metodik a v závislosti na poskytovaných službách tak, aby nedošlo k omezení poskytovaných služeb a zároveň aby služba byla převzata s veškerými důležitými závislostmi na další poskytované služby a aby nedošlo k omezení těchto služeb během přebíracího období.

Oblast poskytování uvedené služby Správa infrastrukturních služeb je základem pro velkou část infrastruktury a proto na této službě je závislá většina dalších katalogových listů jakou jsou Obecné pravidelné služby a SLA, Monitoring a dohledové nástroje, HelpDesk služby, Správa serverové výpočetní infrastruktury SUN Sparc, SUN Enterprise, Správa serverové výpočetní infrastruktury IBM x86, Správa serverové výpočetní infrastruktury IBM POWER, Správa serverové výpočetní infrastruktury HPe, Správa prostředí Managementu, SAN a diskových polí, Správa LAN prvků DC, Správa virtualizační platformy VMware, Správa služby MS Active Directory, Správa služby Certifikační autorita, Správa databázových serverů pro ORACLE, Správa databázových serverů pro MS SQL, Správa databázových serverů pro INFORMIX, Správa služby MS Exchange Server, Správa MS Windows serverů a Linux serverů.

V rámci přebíracího období musí být jasně specifikovány měřitelné parametry dle katalogového listu, pro zajištění vyhodnocování této služby. Jednotlivé parametry SLA budou vyhodnocovány z dohledového nástroje, který tyto parametry eviduje. Tyto měřitelné hodnoty bude obsahovat pravidelný report, ve kterém budou uvedené hodnoty a tím i informace o plnění uvedené služby.

Metodický a procesní postup převzetí služeb

Pro zajištění převzetí uvedené služby bude použita projektová metodika PRINCE2® dle které budou zajištěny veškeré náležitosti, jako jsou:

- Celkové naplánování převzetí služby – seznam dílčích kroků, jejich vzájemných vazeb a termínů zahájení a ukončení

- Definice rizik v převzetí služby
- Koordinace třetích stran a optimalizovat potřebné součinnosti při převzetí služby

Převzetí služby bude dále probíhat dle metodiky ITIL, která zajistí převzetí požadovaných služeb dle definovaných standardů. Použitá metodika bude řešit zejména níže uvedené oblasti.

- Definice požadované služby
- Nastavení služby
- Testovací provoz služby
- Validace služby
- Řízení změn
- Měření služby

Při převzetí služeb je nutné zohlednění metodik a politik v prostředí Zadavatele, a to zejména vydaných metodických pokynů a jednotlivých provozních řádů. Konkrétně se jedná o:

- Politika bezpečnosti informací Magistrátu hl. m. Prahy
- Technická bezpečnostní politika správy ICT
- Technická bezpečnostní politika sítí
- Technická bezpečnostní politika konfigurace ICT
- Instrukce pro přístup do oblastí zajištěných PZTS
- Metodický pokyn č. 7/2017–k řízení bezpečnostních událostí a bezpečnostních incidentů
- Metodický pokyn č. 8/2017 - Pravidla užívání informačního systému Magistrátu hl. m. Prahy
- Metodický pokyn č. 2/2018–k systému řízení IT služeb
- Metodický pokyn č. 1/2019 – Provozní řád datového centra DC4
- Metodický pokyn č. 2/2019 – Provozní řád datového centra DC5

Návrh harmonogramu

Detail činnosti	T+2	T+4	T+6	T+8	T+12	T+16
Příprava plánu převzetí						
Předání a seznámení se s dokumentací						
Předání přístupů k jednotlivým službám						
Provedení analýzy prostředí						
Nastavení návazných procesů - monitoring						
Workshop před převzetím služby						
Převzetí služby						

(T=počty dnů)

Požadovaná součinnost zadavatele

- Dodání dokumentace ke spravovaným službám, prvkům a veškeré související infrastruktury, seznamu souvisejícího HW a SW, seznamu a obsahu procesů.
- Nastavení fyzického i elektronického přístupu k dotčeným systémům pro poskytovatele
- Předání IP adresní plány
- Používaná jména konvence pro DNS
- Seznam DNS zón
- Seznam služeb využívající RADIUS
- Nastavení kontaktních a zodpovědných osob do kontaktní matice, a to včetně kontaktů pro komunikaci s dalšími navazujícími službami
- Stanovení vzoru pravidelného reportingu
- Zajištění VPN přístupu

Analýza rizik v dané oblasti

V rámci analýzy a řízení rizik je potřeba postupovat následujícími kroky „Identifikace" -> „Hodnocení" -> „Implementace". Analýza rizik je prováděna dle odhadnuté pravděpodobnosti a dopadu.

Pro převzetí uvedené služby jsme identifikovaly následující rizika:

Riziko	Hodnocení rizika	Návrh nápravného opatření
Nedodržení časového harmonogramu	Střední	Včasné zajištění veškerých potřebných podkladů a součinností pro převzetí služby
Nedostatečný přístup k informacím pro provedení analýzy	Střední	Včasné předání veškerých potřebných informací a přístupů pro provedení analýzy, správné nastavení komunikační matice
Nedostatečná nebo žádná dokumentace k systémům, případně rozpory mezi dokumentací a skutečným stavem	Střední	Zajistit podporu objednatele, stanovení odpovědnosti na straně objednatele a zajištění potřebných vstupů. Detailní validace dokumentace vůči skutečnosti a případná oprava dokumentace dle stavu.
Nesoučinnost třetích stran	Střední	Včasné kontaktování třetích stran pro zajištění potřebných součinností, stanovení odpovědnosti a rozhodovací pravomoci na

		straně objednatele
Nezajištění fyzického nebo elektronického přístupu k systémům	Nízké	Včasné otevření komunikace o přístupech a všech nutných podmínkách
Nezajištění všech nutných přístupových oprávnění (účtů) k systémům	Nízké	Zajistit včasnou validaci všech účtů a oprávnění nutných pro provedení převzetí i následné poskytování služby
Nesprávné kontakty v komunikační matici	Nízké	Zajistit včasnou validaci všech kontaktů nutných pro provedení převzetí i následné poskytování služby
Poškození dat	Střední	Pro minimalizování rizika je nutné mít zajištěny zálohy dohledového systému
Systémy bez podpory	Střední	Zajištění základní servisní podpory provozovaných systémů

KL11a – Správa databázových serverů pro ORACLE

Popis návrhu převzetí služeb

Před převzetím služby je nutné nejdříve stanovit jasný plán převzetí. Tento plán musí obsahovat: Vymezení hlavních kontaktních osob, definice procesů, způsob omezování rizik, definice akceptačních kritérií a harmonogram převzetí služeb.

Následně bude nutné jasně specifikovat procesy v rámci převzetí služeb, a to zejména v oblasti kontroly změn, kontroly sporných skutečností a kontroly rizik v převzetí služby. Dále bude nutné vytvořit komunikační matici pro nastavení komunikačních kanálů v této oblasti pro zajištění informovanosti při přebíracím období. V rámci přebíracího období bude definován popis Implementačních kritérií, procesu testování a akceptace připravenosti na započetí poskytování cílových služeb. Při převzetí služeb bude zohledněn dopady na zaměstnance koncového zákazníka, dopad na interní procesy a postupy koncového zákazníka, připravenost vybavení, rozhraní a procesů nutných pro bezproblémové zahájení poskytování cílových služeb, finanční a obchodní dopady zahájení poskytování cílových služeb.

Před spuštěním této služby je nejprve nutné provést analýzu této oblasti. Je nutné zajistit detailní dokumentaci k danému prostředí, zejména je nutné zajistit kompletní seznam provozovaných databází, verze jednotlivých MS SQL databází, seznam jednotlivých schémat, seznam administrátorských přístupů, seznam provozovaných aplikací využívající uvedené databáze a seznam kontaktů zodpovědných za dané systémy. Nedílnou součástí této analýzy by mělo být dodání ze strany zadavatele vazby na jednotlivé aplikační systémy z pohledu celé architektury prostředí.

Po dodání těchto informací musí dojít ke kontrole zjištěných skutečností.

Po uvedené analýze musí dojít k vytvoření nových administrátorských přístupů pro možnost správy databází a odebrání původních přístupů.

Následně budou převzaté systémy zaneseny do dokumentace, připraven návrh pravidelných zásahů, zajištěno monitorování systémů a nastavení SLA parametrů pro definované služby. Dále musí dojit k informování dotčených osob o změně poskytovatele těchto služeb.

Během převzetí uvedené služby bude vypracována zpráva, ve které budou uvedeny zjištěné skutečnosti během přebíracího období a zároveň návrh činností pro zkvalitnění dodávané služby.

Následně dojde ke spuštění služby a zároveň k zahájení měření jednotlivých SLA parametrů, které budou pravidelně reportovány.

Přístup k řešení dané oblasti

Převzetí uvedené služby bude stanoveno dle standardních využívaných metodik a v závislosti na poskytovaných službách tak, aby nedošlo k omezení poskytovaných služeb a zároveň aby služba byla převzata s veškerými důležitými závislostmi na další poskytované služby a aby nedošlo k omezení těchto služeb během přebíracího období.

Oblast poskytování uvedené služby Správa databázových serverů pro ORACLE je závislé na Obecné pravidelné služby a SLA, HelpDesk služby, Správa serverové výpočetní infrastruktury SUN Sparc, SUN Enterprise, Správa serverové výpočetní infrastruktury IBM x86, Správa serverové výpočetní infrastruktury HPe, Správa prostředí Managementu, SAN a diskových polí, Správa LAN prvků DC, Správa virtualizační platformy VMware, Správa služby MS Active Directory, Správa služby Certifikační autorita, Správa infrastrukturních služeb, Správa MS Windows serverů a Linux serverů.

V rámci přebíracího období musí být jasně specifikovány měřitelné parametry dle katalogového listu, pro zajištění vyhodnocování této služby. Jednotlivé parametry SLA budou vyhodnocovány z dohledového nástroje, který tyto parametry eviduje. Tyto měřitelné hodnoty bude obsahovat pravidelný report, ve kterém budou uvedené hodnoty a tím i informace o plnění uvedené služby.

Metodický a procesní postup převzetí služeb

Pro zajištění převzetí uvedené služby bude použita projektová metodika PRINCE2® dle které budou zajištěny veškeré náležitosti, jako jsou:

- Celkové naplánování převzetí služby – seznam dílčích kroků, jejich vzájemných vazeb a termínů zahájení a ukončení
- Definice rizik v převzetí služby
- Koordinace třetích stran a optimalizovat potřebné součinnosti při převzetí služby

Převzetí služby bude dále probíhat dle metodiky ITIL, která zajistí převzetí požadovaných služeb dle definovaných standardů. Použitá metodika bude řešit zejména níže uvedené oblasti.

- Definice požadované služby

- Nastavení služby
- Testovací provoz služby
- Validace služby
- Řízení změn
- Měření služby

Při převzetí služeb je nutné zohlednění metodik a politik v prostředí Zadavatele, a to zejména vydaných metodických pokynů a jednotlivých provozních řádů. Konkrétně se jedná o:

- Politika bezpečnosti informací Magistrátu hl. m. Prahy
- Technická bezpečnostní politika správy ICT
- Technická bezpečnostní politika sítí
- Technická bezpečnostní politika konfigurace ICT
- Instrukce pro přístup do oblastí zajištěných PZTS
- Metodický pokyn č. 7/2017–k řízení bezpečnostních událostí a bezpečnostních incidentů
- Metodický pokyn č. 8/2017 - Pravidla užívání informačního systému Magistrátu hl. m. Prahy
- Metodický pokyn č. 2/2018–k systému řízení IT služeb
- Metodický pokyn č. 1/2019 – Provozní řád datového centra DC4
- Metodický pokyn č. 2/2019 – Provozní řád datového centra DC5

Návrh harmonogramu

Detail činnosti	T+2	T+8	T+12	T+16	T+20
Příprava plánu převzetí					
Předání a seznámení se s dokumentací					
Nastavení oprávnění					
Provedení analýzy prostředí					
Ověření licencí					
Nastavení návazných procesů - monitoring					
Workshop před převzetím služby					
Převzetí služby					

(T=počty dnů)

Požadovaná součinnost zadavatele

- Seznam fyzických serverů a jejich umístění
- Nastavení fyzického i elektronického přístupu k dotčeným systémům pro poskytovatele
- Dodání dokumentace Oracle serverů a veškeré související infrastruktury, seznamu souvisejícího HW a SW, seznamu databází a přístupových práv k jednotlivým databázím
- Nastavení kontaktních a zodpovědných osob do kontaktní matice, a to včetně kontaktů pro komunikaci s dalšími navazujícími službami
- Dodání přístupových oprávnění ke všem příslušným systémům
- Stanovení vzoru pravidelného reportingu
- Zajištění VPN přístupu

Analýza rizik v dané oblasti

V rámci analýzy a řízení rizik je potřeba postupovat následujícími kroky „Identifikace" -> „Hodnocení" -> „Implementace". Analýza rizik je prováděna dle odhadnuté pravděpodobnosti a dopadu.

Pro převzetí uvedené služby jsme identifikovaly následující rizika:

Riziko	Hodnocení rizika	Návrh nápravného opatření
Nedodržení časového harmonogramu	Střední	Včasné zajištění veškerých potřebných podkladů a součinností pro převzetí služby
Nedostatečný přístup k informacím pro provedení analýzy	Střední	Včasné předání veškerých potřebných informací a přístupů pro provedení analýzy, správné nastavení komunikační matice
Nedostatečná nebo žádná dokumentace k systémům	Střední	Zajistit podporu objednatele, stanovení odpovědnosti na straně objednatele a zajištění potřebných vstupů. Detailní validace dokumentace vůči skutečnosti.
Nesoučinnost třetích stran	Střední	Včasné kontaktování třetích stran pro zajištění potřebných součinností, stanovení odpovědnosti a rozhodovací pravomoci na straně objednatele
Nedostatečné informace o zálohovacím řešení	Nízké	Zajistit podporu objednatele, stanovení odpovědnosti na straně objednatele
Nezajištění fyzického nebo elektronického přístupu k systémům	Nízké	Včasné otevření komunikace o přístupech a všech nutných podmínkách
Nezajištění všech nutných přístupových oprávnění (účtů) k systémům	Nízké	Zajistit včasnou validaci všech účtů a oprávnění nutných pro provedení převzetí i následné poskytování služby
Nesprávné kontakty v komunikační matici	Nízké	Zajistit včasnou validaci všech kontaktů nutných pro provedení převzetí i následné poskytování služby

Chybějící návaznost na ostatní služby a chybějící kontakt pro případ potřeby.	Nízké	Ověřit všechny vazby ostatních služeb na zálohování. Zajistit a validovat kontakty u všech navazujících služeb, které budou v případě potřeby spolupracovat
Poškození dat	Střední	Pro minimalizování rizika je nutné mít zajištěny zálohy dohledového systému
Systémy bez podpory	Střední	Zajištění základní servisní podpory provozovaných systémů

KL11b – Správa databázových serverů pro MS SQL

Popis návrhu převzetí služeb

Před převzetím služby je nutné nejdříve stanovit jasný plán převzetí. Tento plán musí obsahovat: Vymezení hlavních kontaktních osob, definice procesů, způsob omezování rizik, definice akceptačních kritérií a harmonogram převzetí služeb.

Následně bude nutné jasně specifikovat procesy v rámci převzetí služeb, a to zejména v oblasti kontroly změn, kontroly sporných skutečností a kontroly rizik v převzetí služby. Dále bude nutné vytvořit komunikační matici pro nastavení komunikačních kanálů v této oblasti pro zajištění informovanosti při přebíracím období. V rámci přebíracího období bude definován popis Implementačních kritérií, procesu testování a akceptace připravenosti na započetí poskytování cílových služeb. Při převzetí služeb bude zohledněn dopady na zaměstnance koncového zákazníka, dopad na interní procesy a postupy koncového zákazníka, připravenost vybavení, rozhraní a procesů nutných pro bezproblémové zahájení poskytování cílových služeb, finanční a obchodní dopady zahájení poskytování cílových služeb.

Před spuštěním této služby je nejprve nutné provést analýzu této oblasti. Je nutné zajistit detailní dokumentaci k danému prostředí, zejména je nutné zajistit kompletní seznam provozovaných databází, verze jednotlivých MS SQL databází, seznam jednotlivých schémat, seznam administrátorských přístupů, seznam provozovaných aplikací využívající uvedené databáze a seznam kontaktů zodpovědných za dané systémy. Nedílnou součástí této analýzy by mělo být dodání ze strany zadavatele vazby na jednotlivé aplikační systémy z pohledu celé architektury prostředí.

Po dodání těchto informací musí dojít ke kontrole zjištěných skutečností.

Po uvedené analýze musí dojít k vytvoření nových administrátorských přístupů pro možnost správy databází a odebrání původních přístupů.

Následně budou převzaté systémy zaneseny do dokumentace, připraven návrh pravidelných zásahů, zajištěno monitorování systémů a nastavení SLA parametrů pro definované služby. Dále musí dojít k informování dotčených osob o změně poskytovatele těchto služeb.

Během převzetí uvedené služby bude vypracována zpráva, ve které budou uvedeny zjištěné skutečnosti během přebíracího období a zároveň návrh činností pro zkvalitnění dodávané služby.

Následně dojde ke spuštění služby a zároveň k zahájení měření jednotlivých SLA parametrů, které budou pravidelně reportovány.

Přístup k řešení dané oblasti

Převzetí uvedené služby bude stanoveno dle standardních využívaných metodik a v závislosti na poskytovaných službách tak, aby nedošlo k omezení poskytovaných služeb a zároveň aby služba byla převzata s veškerými důležitými závislostmi na další poskytované služby a aby nedošlo k omezení těchto služeb během přebíracího období

Oblast poskytování uvedené služby Správa databázových serverů pro MS SQL je závislé na Obecné pravidelné služby a SLA, HelpDesk služby, Správa serverové výpočetní infrastruktury IBM x86, Správa serverové výpočetní infrastruktury HPe, Správa prostředí Managementu, SAN a diskových polí, Správa LAN prvků DC, Správa virtualizační platformy VMware, Správa služby MS Active Directory, Správa služby Certifikační autorita, Správa infrastrukturních služeb, Správa MS Windows serverů a Linux serverů.

V rámci přebíracího období musí být jasně specifikovány měřitelné parametry dle katalogového listu, pro zajištění vyhodnocování této služby. Jednotlivé parametry SLA budou vyhodnocovány z dohledového nástroje, který tyto parametry eviduje. Tyto měřitelné hodnoty bude obsahovat pravidelný report, ve kterém budou uvedené hodnoty a tím i informace o plnění uvedené služby.

Metodický a procesní postup převzetí služeb

Pro zajištění převzetí uvedené služby bude použita projektová metodika PRINCE2® dle které budou zajištěny veškeré náležitosti, jako jsou:

- Celkové naplánování převzetí služby – seznam dílčích kroků, jejich vzájemných vazeb a termínů zahájení a ukončení
- Definice rizik v převzetí služby
- Koordinace třetích stran a optimalizovat potřebné součinnosti při převzetí služby

Převzetí služby bude dále probíhat dle metodiky ITIL, která zajistí převzetí požadovaných služeb dle definovaných standardů. Použitá metodika bude řešit zejména níže uvedené oblasti.

- Definice požadované služby
- Nastavení služby
- Testovací provoz služby
- Validace služby
- Řízení změn

- Měření služby

Při převzetí služeb je nutné zohlednění metodik a politik v prostředí Zadavatele, a to zejména vydaných metodických pokynů a jednotlivých provozních řádů. Konkrétně se jedná o:

- Politika bezpečnosti informací Magistrátu hl. m. Prahy
- Technická bezpečnostní politika správy ICT
- Technická bezpečnostní politika sítí
- Technická bezpečnostní politika konfigurace ICT
- Instrukce pro přístup do oblastí zajištěných PZTS
- Metodický pokyn č. 7/2017–k řízení bezpečnostních událostí a bezpečnostních incidentů
- Metodický pokyn č. 8/2017 - Pravidla užívání informačního systému Magistrátu hl. m. Prahy
- Metodický pokyn č. 2/2018–k systému řízení IT služeb
- Metodický pokyn č. 1/2019 – Provozní řád datového centra DC4
- Metodický pokyn č. 2/2019 – Provozní řád datového centra DC5

Návrh harmonogramu

Detail činnosti	T+2	T+8	T+12	T+16	T+20
Příprava plánu převzetí					
Předání a seznámení se s dokumentací					
Nastavení oprávnění					
Provedení analýzy prostředí					
Ověření licencí					
Nastavení návazných procesů - monitoring					
Workshop před převzetím služby					
Převzetí služby					

(T=počty dnů)

Požadovaná součinnost zadavatele

- Seznam fyzických serverů a jejich umístění
- Nastavení fyzického i elektronického přístupu k dotčeným systémům pro poskytovatele
- Dodání dokumentace MS SQL serverů a veškeré související infrastruktury, seznamu souvisejícího HW a SW, seznamu databází a přístupových práv k jednotlivým SQL instancím a databázím
- Nastavení kontaktních a zodpovědných osob do kontaktní matice, a to včetně kontaktů pro komunikaci s dalšími navazujícími službami
- Dodání přístupových oprávnění ke všem příslušným systémům
- Stanovení vzoru pravidelného reportingu
- Zajištění VPN přístupu

Analýza rizik v dané oblasti

V rámci analýzy a řízení rizik je potřeba postupovat následujícími kroky „Identifikace" -> „Hodnocení" -> „Implementace". Analýza rizik je prováděna dle odhadnuté pravděpodobnosti a dopadu.

Pro převzetí uvedené služby jsme identifikovaly následující rizika:

Riziko	Hodnocení rizika	Návrh nápravného opatření
Nedodržení časového harmonogramu	Střední	Včasné zajištění veškerých potřebných podkladů a součinností pro převzetí služby
Nedostatečný přístup k informacím pro provedení analýzy	Střední	Včasné předání veškerých potřebných informací a přístupů pro provedení analýzy, správné nastavení komunikační matice
Nedostatečná nebo žádná dokumentace k systémům	Střední	Zajistit podporu objednatele, stanovení odpovědnosti na straně objednatele a zajištění potřebných vstupů. Detailní validace dokumentace vůči skutečnosti.
Nesoučinnost třetích stran	Střední	Včasné kontaktování třetích stran pro zajištění potřebných součinností, stanovení odpovědnosti a rozhodovací pravomoci na straně objednatele
Nedostatečné informace o MS SQL řešení	Nízké	Zajistit podporu objednatele, stanovení odpovědnosti na straně objednatele
Nezajištění fyzického nebo elektronického přístupu k systémům	Nízké	Včasné otevření komunikace o přístupech a všech nutných podmínkách
Nezajištění všech nutných přístupových oprávnění (účtů) k systémům	Nízké	Zajistit včasnou validaci všech účtů a oprávnění nutných pro provedení převzetí i následné poskytování služby
Nesprávné kontakty v komunikační matici	Nízké	Zajistit včasnou validaci všech kontaktů nutných pro provedení převzetí i následné poskytování služby
Chybějící návaznost na	Nízké	Ověřit všechny vazby

ostatní služby a chybějící kontakt pro případ potřeby.		ostatních služeb na MS SQL. Zajistit a validovat kontakty u všech navazujících služeb, které budou v případě potřeby spolupracovat
Poškození dat	Střední	Pro minimalizování rizika je nutné mít zajištěny zálohy dohledového systému
Systémy bez podpory	Střední	Zajištění základní servisní podpory provozovaných systémů

KL11c – Správa databázových serverů pro INFORMIX

Popis návrhu převzetí služeb

Před převzetím služby je nutné nejdříve stanovit jasný plán převzetí. Tento plán musí obsahovat: Vymezení hlavních kontaktních osob, definice procesů, způsob omezování rizik, definice akceptačních kritérií a harmonogram převzetí služeb.

Následně bude nutné jasně specifikovat procesy v rámci převzetí služeb, a to zejména v oblasti kontroly změn, kontroly sporných skutečností a kontroly rizik v převzetí služby. Dále bude nutné vytvořit komunikační matici pro nastavení komunikačních kanálů v této oblasti pro zajištění informovanosti při přebíracím období. V rámci přebíracího období bude definován popis Implementačních kritérií, procesu testování a akceptace připravenosti na započetí poskytování cílových služeb. Při převzetí služeb bude zohledněn dopady na zaměstnance koncového zákazníka, dopad na interní procesy a postupy koncového zákazníka, připravenost vybavení, rozhraní a procesů nutných pro bezproblémové zahájení poskytování cílových služeb, finanční a obchodní dopady zahájení poskytování cílových služeb.

Před spuštěním této služby je nejprve nutné provést analýzu této oblasti. Je nutné zajistit detailní dokumentaci k danému prostředí, zejména je nutné zajistit kompletní seznam provozovaných databází, verze jednotlivých schémat, seznam administrátorských přístupů, seznam provozovaných aplikací využívající uvedené databáze a seznam kontaktů zodpovědných za dané systémy. Nedílnou součástí této analýzy by mělo být dodání ze strany zadavatele vazby na jednotlivé aplikační systémy z pohledu celé architektury prostředí.

Po dodání těchto informací musí dojít ke kontrole zjištěných skutečností.

Po uvedené analýze musí dojít k vytvoření nových administrátorských přístupů pro možnost správy databází a odebrání původních přístupů.

Následně budou převzaté systémy zaneseny do dokumentace, připraven návrh pravidelných zásahů, zajištěno monitorování systémů a nastavení SLA parametrů pro definované služby. Dále musí dojít k informování dotčených osob o změně poskytovatele těchto služeb.

Během převzetí uvedené služby bude vypracována zpráva, ve které budou uvedeny zjištěné skutečnosti během přebíracího období a zároveň návrh činností pro zkvalitnění dodávané služby.

Následně dojde ke spuštění služby a zároveň k zahájení měření jednotlivých SLA parametrů, které budou pravidelně reportovány.

Přístup k řešení dané oblasti

Převzetí uvedené služby bude stanoveno dle standardních využívaných metodik a v závislosti na poskytovaných službách tak, aby nedošlo k omezení poskytovaných služeb a zároveň aby služba byla převzata s veškerými důležitými závislostmi na další poskytované služby a aby nedošlo k omezení těchto služeb během přebíracího období.

Oblast poskytování uvedené služby Správa databázových serverů pro INFORMIX je závislé na Obecné pravidelné služby a SLA, HelpDesk služby, Správa serverové výpočetní infrastruktury SUN Sparc, SUN Enterprise, Správa serverové výpočetní infrastruktury IBM x86, Správa serverové výpočetní infrastruktury HPe, Správa prostředí Managementu, SAN a diskových polí, Správa LAN prvků DC, Správa virtualizační platformy VMware, Správa služby MS Active Directory, Správa služby Certifikační autorita, Správa infrastrukturních služeb, Správa MS Windows serverů a Linux serverů.

V rámci přebíracího období musí být jasně specifikovány měřitelné parametry dle katalogového listu, pro zajištění vyhodnocování této služby. Jednotlivé parametry SLA budou vyhodnocovány z dohledového nástroje, který tyto parametry eviduje. Tyto měřitelné hodnoty bude obsahovat pravidelný report, ve kterém budou uvedené hodnoty a tím i informace o plnění uvedené služby.

Metodický a procesní postup převzetí služeb

Pro zajištění převzetí uvedené služby bude použita projektová metodika PRINCE2® dle které budou zajištěny veškeré náležitosti, jako jsou:

- Celkové naplánování převzetí služby – seznam dílčích kroků, jejich vzájemných vazeb a termínů zahájení a ukončení
- Definice rizik v převzetí služby
- Koordinace třetích stran a optimalizovat potřebné součinnosti při převzetí služby

Převzetí služby bude dále probíhat dle metodiky ITIL, která zajistí převzetí požadovaných služeb dle definovaných standardů. Použitá metodika bude řešit zejména níže uvedené oblasti.

- Definice požadované služby
- Nastavení služby
- Testovací provoz služby
- Validace služby
- Řízení změn
- Měření služby

Při převzetí služeb je nutné zohlednění metodik a politik v prostředí Zadavatele, a to zejména vydaných metodických pokynů a jednotlivých provozních řádů. Konkrétně se jedná o:

- Politika bezpečnosti informací Magistrátu hl. m. Prahy
- Technická bezpečnostní politika správy ICT
- Technická bezpečnostní politika sítí
- Technická bezpečnostní politika konfigurace ICT
- Instrukce pro přístup do oblastí zajištěných PZTS
- Metodický pokyn č. 7/2017–k řízení bezpečnostních událostí a bezpečnostních incidentů
- Metodický pokyn č. 8/2017 - Pravidla užívání informačního systému Magistrátu hl. m. Prahy
- Metodický pokyn č. 2/2018–k systému řízení IT služeb
- Metodický pokyn č. 1/2019 – Provozní řád datového centra DC4
- Metodický pokyn č. 2/2019 – Provozní řád datového centra DC5

Návrh harmonogramu

Detail činnosti	T+2	T+6	T+8	T+10	T+12
Příprava plánu převzetí					
Předání a seznámení se s dokumentací					
Nastavení oprávnění					
Provedení analýzy prostředí					
Ověření licencí					
Nastavení návazných procesů - monitoring					
Workshop před převzetím služby					
Převzetí služby					

(T=počty dnů)

Požadovaná součinnost zadavatele

- Seznam fyzických serverů a jejich umístění
- Nastavení fyzického i elektronického přístupu k dotčeným systémům pro poskytovatele
- Dodání dokumentace Informix serverů a veškeré související infrastruktury, seznamu souvisejícího HW a SW, seznamu databází a přístupových práv k jednotlivým databázím
- Nastavení kontaktních a zodpovědných osob do kontaktní matice, a to včetně kontaktů pro komunikaci s dalšími navazujícími službami
- Dodání přístupových oprávnění ke všem příslušným systémům
- Stanovení vzoru pravidelného reportingu
- Zajištění VPN přístupu

Analýza rizik v dané oblasti

V rámci analýzy a řízení rizik je potřeba postupovat následujícími kroky „Identifikace" -> „Hodnocení" -> „Implementace" Analýza rizik je prováděna dle odhadnuté pravděpodobnosti a dopadu.

Pro převzetí uvedené služby jsme identifikovaly následující rizika:

Riziko	Hodnocení rizika	Návrh nápravného opatření
Nedodržení časového harmonogramu	Střední	Včasné zajištění veškerých potřebných podkladů a součinností pro převzetí služby
Nedostatečný přístup k informacím pro provedení analýzy	Střední	Včasné předání veškerých potřebných informací a přístupů pro provedení analýzy, správné nastavení komunikační matice
Nedostatečná nebo žádná dokumentace k systémům	Střední	Zajistit podporu objednatele, stanovení odpovědnosti na straně objednatele a zajištění potřebných vstupů. Detailní validace dokumentace vůči skutečnosti.
Nesoučinnost třetích stran	Střední	Včasné kontaktování třetích stran pro zajištění potřebných součinností, stanovení odpovědnosti a rozhodovací pravomoci na straně objednatele
Nedostatečné informace o zálohovacím řešení	Nízké	Zajistit podporu objednatele, stanovení odpovědnosti na straně objednatele
Nezajištění fyzického nebo elektronického přístupu k systémům	Nízké	Včasné otevření komunikace o přístupech a všech nutných podmínkách
Nezajištění všech nutných přístupových oprávnění (účtů) k systémům	Nízké	Zajistit včasnou validaci všech účtů a oprávnění nutných pro provedení převzetí i následné poskytování služby
Nesprávné kontakty v komunikační matici	Nízké	Zajistit včasnou validaci všech kontaktů nutných pro provedení převzetí i následné poskytování služby
Chybějící návaznost na ostatní služby a chybějící kontakt pro případ potřeby.	Nízké	Ověřit všechny vazby ostatních služeb na zálohování. Zajistit a validovat kontakty u všech navazujících služeb, které budou v případě potřeby spolupracovat

Systémy bez podpory	Vysoké	Zajištění základní servisní podpory provozovaných systémů

KL12 – Správa služby MS Exchange Server

Popis návrhu převzetí služeb

Před převzetím služby je nutné nejdříve stanovit jasný plán převzetí. Tento plán musí obsahovat: Vymezení hlavních kontaktních osob, definice procesů, způsob omezování rizik, definice akceptačních kritérií a harmonogram převzetí služeb.

Následně bude nutné jasně specifikovat procesy v rámci převzetí služeb, a to zejména v oblasti kontroly změn, kontroly sporných skutečností a kontroly rizik v převzetí služby. Dále bude nutné vytvořit komunikační matici pro nastavení komunikačních kanálů v této oblasti pro zajištění informovanosti při přebíracím období. V rámci přebíracího období bude definován popis Implementačních kritérií, procesu testování a akceptace připravenosti na započetí poskytování cílových služeb. Při převzetí služeb bude zohledněn dopady na zaměstnance koncového zákazníka, dopad na interní procesy a postupy koncového zákazníka, připravenost vybavení, rozhraní a procesů nutných pro bezproblémové zahájení poskytování cílových služeb, finanční a obchodní dopady zahájení poskytování cílových služeb.

V rámci přebíracího období dojde ke kontrole jednotlivých Exchange serverů a jednotlivého nastavení všech souvisejících služeb. Dále musí dojít ke kontrole jednotlivých využívaných šablon a kontrola nastavení uživatelských politik. Dojde prověření celkové architektury řešení ve vztahu k označení jako významného informačního systému.

Převzetí služby bude spojené s postupným převzetím dalších souvisejících katalogových listů tak, aby byla zajištěno plnění služby a celkového SLA.

Při převzetí služby bude nastaven pravidelný reporting, který bude obsahovat informace a plnění služby dle nastavených hodnot SLA. Dále bude nastavena komunikační matice pro službu tak, aby vhodné zodpovědné osoby objednatele měly včasné informace o stavu služby a zároveň byly v případě potřeby dostupné pro poskytnutí součinnosti.

Přístup k řešení dané oblasti

Převzetí uvedené služby bude stanoveno dle standardních využívaných metodik a v závislosti na poskytovaných službách tak, aby nedošlo k omezení poskytovaných služeb a zároveň aby služba byla převzata s veškerými důležitými závislostmi na další poskytované služby a aby nedošlo k omezení těchto služeb během přebíracího období.

Oblast poskytování uvedené služby Správa MS Exchange je závislé na Obecné pravidelné služby a SLA, Monitoring a Dohledové nástroje, HelpDesk služby, Správa serverové výpočetní infrastruktury HPe, Správa prostředí Managementu, SAN a diskových polí, Správa LAN prvků DC, Správa virtualizační platformy VMware, Správa služby MS Active Directory, Správa služby

Certifikační autorita, Správa infrastrukturních služeb, Správa MS Windows serverů a Linux serverů.

V rámci přebíracího období musí být jasně specifikovány měřitelné parametry dle katalogového listu, pro zajištění vyhodnocování této služby. Jednotlivé parametry SLA budou vyhodnocovány z dohledového nástroje, který tyto parametry eviduje. Tyto měřitelné hodnoty bude obsahovat pravidelný report, ve kterém budou uvedené hodnoty a tím i informace o plnění uvedené služby.

Metodický a procesní postup převzetí služeb

Pro zajištění převzetí uvedené služby bude použita projektová metodika PRINCE2® dle které budou zajištěny veškeré náležitosti, jako jsou:

- Celkové naplánování převzetí služby – seznam dílčích kroků, jejich vzájemných vazeb a termínů zahájení a ukončení.
- Definice rizik v převzetí služby
- Koordinace třetích stran a optimalizovat potřebné součinnosti při převzetí služby.

Převzetí služby bude dále probíhat dle metodiky ITIL, která zajistí převzetí požadovaných služeb dle definovaných standardů. Použitá metodika bude řešit zejména níže uvedené oblasti.

- Definice požadované služby
- Nastavení služby
- Testovací provoz služby
- Validace služby
- Řízení změn
- Měření služby

Při převzetí služeb je nutné zohlednění metodik a politik v prostředí Zadavatele, a to zejména vydaných metodických pokynů a jednotlivých provozních řádů. Konkrétně se jedná o:

- Politika bezpečnosti informací Magistrátu hl. m. Prahy
- Technická bezpečnostní politika správy ICT
- Technická bezpečnostní politika sítí
- Technická bezpečnostní politika konfigurace ICT
- Instrukce pro přístup do oblastí zajištěných PZTS
- Metodický pokyn č. 7/2017–k řízení bezpečnostních událostí a bezpečnostních incidentů
- Metodický pokyn č. 8/2017 - Pravidla užívání informačního systému Magistrátu hl. m. Prahy
- Metodický pokyn č. 2/2018–k systému řízení IT služeb
- Metodický pokyn č. 1/2019 – Provozní řád datového centra DC4
- Metodický pokyn č. 2/2019 – Provozní řád datového centra DC5

Návrh harmonogramu

Detail činnosti	T+2	T+4	T+6	T+8	T+10	T+14
Příprava plánu převzetí						
Předání a seznámení se s dokumentací						

Nastavení oprávnění						
Provedení analýzy prostředí						
Kontrola prostředí MS Exchage						
Nastavení návazných procesů - monitoring						
Workshop před převzetím služby						
Převzetí služby						

(T=počty dnů)

Požadovaná součinnost zadavatele

- Seznam fyzických serverů a jejich umístění
- Nastavení fyzického i elektronického přístupu k dotčeným systémům pro poskytovatele
- Dodání dokumentace služby MS Exchange server a veškeré související infrastruktury, seznamu souvisejícího HW a SW a procesů přímo navazujících na poštovní služby
- Nastavení kontaktních a zodpovědných osob do kontaktní matice, a to včetně kontaktů pro komunikaci s dalšími navazujícími službami
- Dodání přístupových oprávnění ke všem příslušným systémům
- Stanovení vzoru pravidelného reportingu
- Zajištění VPN přístupu

Analýza rizik v dané oblasti

V rámci analýzy a řízení rizik je potřeba postupovat následujícími kroky „Identifikace" -> „Hodnocení" -> „Implementace". Analýza rizik je prováděna dle odhadnuté pravděpodobnosti a dopadu.

Pro převzetí uvedené služby jsme identifikovaly následující rizika:

Riziko	Hodnocení rizika	Návrh nápravného opatření
Nedodržení časového harmonogramu	Střední	Včasné zajištění veškerých potřebných podkladů a součinností pro převzetí služby
Nedostatečný přístup k informacím pro provedení analýzy	Střední	Včasné předání veškerých potřebných informací a přístupů pro provedení analýzy
Nedostatečná nebo žádná dokumentace k provozovaným systémům	Střední	Zajistit podporu Zadavatele pro optimalizaci, stanovení odpovědnosti na straně Zadavatele a zajištění potřebných vstupů
Poškození dat	Střední	Pro minimalizování rizika je nutné mít zajištěny zálohy dohledového systému
Nesoučinnost třetích stran	Střední	Včasné kontaktování třetích stran pro zajištění potřebných součinností

Nedostatečné informace o řešení poštovních služeb	Nízké	Zajistit podporu objednatele, stanovení odpovědnosti na straně objednatele
Nezajištění fyzického nebo elektronického přístupu k systémům	Nízké	Včasné otevření komunikace o přístupech a všech nutných podmínkách
Nezajištění všech nutných přístupových oprávnění (účtů) k systémům	Nízké	Zajistit včasnou validaci všech účtů a oprávnění nutných pro provedení převzetí i následné poskytování služby
Nesprávné kontakty v komunikační matici	Nízké	Zajistit včasnou validaci všech kontaktů nutných pro provedení převzetí i následné poskytování služby
Chybějící návaznost na ostatní služby a chybějící kontakt pro případ potřeby.	Nízké	Ověřit všechny vazby ostatních služeb na službu Exchange. Zajistit a validovat kontakty u všech navazujících služeb, které budou v případě potřeby spolupracovat
Systémy bez podpory	Střední	Zajištění základní servisní podpory provozovaných systémů

KL13 – Správa MS Windows serverů a Linux serverů

Popis návrhu převzetí služeb

Před převzetím služby je nutné nejdříve stanovit jasný plán převzetí. Tento plán musí obsahovat: Vymezení hlavních kontaktních osob, definice procesů, způsob omezování rizik, definice akceptačních kritérií a harmonogram převzetí služeb.

Následně bude nutné jasně specifikovat procesy v rámci převzetí služeb, a to zejména v oblasti kontroly změn, kontroly sporných skutečností a kontroly rizik v převzetí služby. Dále bude nutné vytvořit komunikační matici pro nastavení komunikačních kanálů v této oblasti pro zajištění informovanosti při přebíracím období. V rámci přebíracího období bude definován popis Implementačních kritérií, procesu testování a akceptace připravenosti na započetí poskytování cílových služeb. Při převzetí služeb bude zohledněn dopady na zaměstnance koncového zákazníka, dopad na interní procesy a postupy koncového zákazníka, připravenost vybavení, rozhraní a procesů nutných pro bezproblémové zahájení poskytování cílových služeb, finanční a obchodní dopady zahájení poskytování cílových služeb.

V rámci přebíracího období musí dojít k převzetí dokumentace ke spravovaným serverům, přístupových oprávněních k systémům a servisních účtů, kontrole monitorovaných systémů v závislosti na dodaném seznamu spravovaných serverů, kontrole dodané dokumentace a celkové architektuře aplikací v závislosti na serverech a určení kritických systémů. Dále musí být stanovena komunikační matice za jednotlivé systém/aplikace a to jak ze strany dodavatele, tak i ze strany technického garanta.

Následně budou převzaté systémy zaneseny do dokumentace, připraven návrh pravidelných zásahů, zajištěno monitorování systémů a nastavení SLA parametrů pro definované služby. Dále musí dojít k informování dotčených osob o změně poskytovatele těchto služeb.

Po těchto krocích dojde k převzetí uvedené služby.

Přístup k řešení dané oblasti

Převzetí uvedené služby bude stanoveno dle standardních využívaných metodik a v závislosti na poskytovaných službách tak, aby nedošlo k omezení poskytovaných služeb a zároveň aby služba byla převzata s veškerými důležitými závislostmi na další poskytované služby a aby nedošlo k omezení těchto služeb během přebíracího období.

Oblast poskytování uvedené služby Správa MS Windows a Linux serverů je závislé na Obecné pravidelné služby a SLA, Monitoring a Dohledové služby, HelpDesk služby, Správa serverové výpočetní infrastruktury SUN Sparc, SUN Enterprise, Správa serverové výpočetní infrastruktury IBM x86, Správa serverové výpočetní infrastruktury IBM POWER, Správa serverové výpočetní infrastruktury HPe, Správa prostředí Managementu, SAN a diskových polí, Správa LAN prvků DC, Správa virtualizační platformy VMware, Správa služby MS Active Directory, Správa služby Certifikační autorita, Správa infrastrukturních služeb, Správa databázových serverů pro ORACLE, Správa databázových serverů pro MS SQL, Správa databázových serverů pro INFORMIX, Správa služby MS Exchange Server.

V rámci přebíracího období musí být jasně specifikovány měřitelné parametry dle katalogového listu, pro zajištění vyhodnocování této služby. Jednotlivé parametry SLA budou vyhodnocovány z dohledového nástroje, který tyto parametry eviduje a z nástroje Helpdesk. Tyto měřitelné hodnoty bude obsahovat pravidelný report, ve kterém budou uvedené hodnoty a tím i informace o plnění uvedené služby.

Metodický a procesní postup převzetí služeb

Pro zajištění převzetí uvedené služby bude použita projektová metodika PRINCE2® dle které budou zajištěny veškeré náležitosti, jako jsou:

- Celkové naplánování převzetí služby – seznam dílčích kroků, jejich vzájemných vazeb a termínů zahájení a ukončení
- Definice rizik v převzetí služby
- Koordinace třetích stran a optimalizovat potřebné součinnosti při převzetí služby

Převzetí služby bude dále probíhat dle metodiky ITIL, která zajistí převzetí požadovaných služeb dle definovaných standardů. Použitá metodika bude řešit zejména níže uvedené oblasti.

- Definice požadované služby

- Nastavení služby
- Testovací provoz služby
- Validace služby
- Řízení změn
- Měření služby

Při převzetí služeb je nutné zohlednění metodik a politik v prostředí Zadavatele, a to zejména vydaných metodických pokynů a jednotlivých provozních řádů. Konkrétně se jedná o:

- Politika bezpečnosti informací Magistrátu hl. m. Prahy
- Technická bezpečnostní politika správy ICT
- Technická bezpečnostní politika sítí
- Technická bezpečnostní politika konfigurace ICT
- Instrukce pro přístup do oblastí zajištěných PZTS
- Metodický pokyn č. 7/2017–k řízení bezpečnostních událostí a bezpečnostních incidentů
- Metodický pokyn č. 8/2017 - Pravidla užívání informačního systému Magistrátu hl. m. Prahy
- Metodický pokyn č. 2/2018–k systému řízení IT služeb
- Metodický pokyn č. 1/2019 – Provozní řád datového centra DC4
- Metodický pokyn č. 2/2019 – Provozní řád datového centra DC5

Návrh harmonogramu

Detail činnosti	T+2	T+4	T+6	T+10	T+12	T+16
Příprava plánu převzetí						
Předání a seznámení se s dokumentací						
Nastavení oprávnění						
Provedení analýzy prostředí						
Kontrola prostředí jednotlivých serverů						
Ověření licencí						
Nastavení návazných procesů - monitoring						
Workshop před převzetím služby						
Převzetí služby						

(T=počty dnů)

Požadovaná součinnost zadavatele

- Seznam fyzických serverů a jejich umístění
- Detailní informace ke každému serveru
  - kompletní konfigurace všech součástí serverů
  - stavy záruk
  - Verze instalovaného operačního systému
  - Přístupové oprávnění na management těchto serverů
- Seznam aplikací, které jsou provozovány na serverech a seznam administrátorů zodpovědných za aplikace
- Nastavení fyzického i elektronického přístupu k dotčeným systémům pro poskytovatele

- Dodání dokumentace ke spravovaným serverům a veškeré související infrastruktury, seznamu souvisejícího HW a SW, seznamu a obsahu procesů
- Nastavení kontaktních a zodpovědných osob do kontaktní matice, a to včetně kontaktů pro komunikaci s dalšími navazujícími službami
- Stanovení vzoru pravidelného reportingu
- Zajištění VPN přístupu

Analýza rizik v dané oblasti

V rámci analýzy a řízení rizik je potřeba postupovat následujícími kroky „Identifikace" -> „Hodnocení" -> „Implementace". Analýza rizik je prováděna dle odhadnuté pravděpodobnosti a dopadu.

Pro převzetí uvedené služby jsme identifikovaly následující rizika:

Riziko	Hodnocení rizika	Návrh nápravného opatření
Nedodržení časového harmonogramu	Střední	Včasné zajištění veškerých potřebných podkladů a součinností pro převzetí služby
Nedostatečný přístup k informacím pro provedení analýzy	Střední	Včasné předání veškerých potřebných informací a přístupů pro provedení analýzy
Nedostatečná nebo žádná dokumentace k provozovaným systémům	Střední	Zajistit podporu Zadavatele pro optimalizaci, stanovení odpovědnosti na straně Zadavatele a zajištění potřebných vstupů
Poškození dat	Střední	Pro minimalizování rizika je nutné mít zajištěny zálohy dohledového systému
Nesoučinnost třetích stran	Střední	Včasné kontaktování třetích stran pro zajištění potřebných součinností
Nezajištění fyzického nebo elektronického přístupu k systémům	Nízké	Včasné otevření komunikace o přístupech a všech nutných podmínkách
Nezajištění všech nutných přístupových oprávnění (účtů) k systémům	Nízké	Zajistit včasnou validaci všech účtů a oprávnění nutných pro provedení převzetí i následné poskytování služby
Nesprávné kontakty v komunikační matici	Nízké	Zajistit včasnou validaci všech kontaktů nutných pro provedení převzetí i následné poskytování služby
Systémy bez podpory	Střední	Zajištění základní servisní podpory provozovaných

		systémů

KL14 – Správa zálohování

Popis návrhu převzetí služeb

Před převzetím služby je nutné nejdříve stanovit jasný plán převzetí. Tento plán musí obsahovat: Vymezení hlavních kontaktních osob, definice procesů, způsob omezování rizik, definice akceptačních kritérií a harmonogram převzetí služeb.

Následně bude nutné jasně specifikovat procesy v rámci převzetí služeb, a to zejména v oblasti kontroly změn, kontroly sporných skutečností a kontroly rizik v převzetí služby. Dále bude nutné vytvořit komunikační matici pro nastavení komunikačních kanálů v této oblasti pro zajištění informovanosti při přebíracím období. V rámci přebíracího období bude definován popis Implementačních kritérií, procesu testování a akceptace připravenosti na započetí poskytování cílových služeb. Při převzetí služeb bude zohledněn dopady na zaměstnance koncového zákazníka, dopad na interní procesy a postupy koncového zákazníka, připravenost vybavení, rozhraní a procesů nutných pro bezproblémové zahájení poskytování cílových služeb, finanční a obchodní dopady zahájení poskytování cílových služeb.

Převzetí služby bude spojené s postupným převzetím dalších katalogových listů tak, aby bylo zajištěno plnění služby, ale také ostatních provázaných služeb a celkového SLA.

V rámci přebíracího období bude zkontrolován současný stav zálohování a nadefinované politiky zálohování. Dále bude zkontrolován stav zálohovaných a nezálohovaných systémů dle požadavku zadavatele.

Při převzetí této služby bude nastaven pravidelný reporting, který bude obsahovat informace o plnění služby dle nastavených hodnot SLA. Dále bude nastavena kontaktní a komunikační matice pro službu tak, aby vhodné zodpovědné osoby objednatele měly včasné informace o stavu služby a zároveň byly v případě potřeby dostupné pro poskytnutí součinnosti.

Přístup k řešení dané oblasti

Převzetí uvedené služby bude stanoveno dle standardních využívaných metodik a v závislosti na poskytovaných službách tak, aby nedošlo k omezení poskytovaných služeb a zároveň aby služba byla převzata s veškerými důležitými závislostmi na další poskytované služby a aby nedošlo k omezení těchto služeb během přebíracího období.

Oblast poskytování uvedené služby Správa zálohování je závislé na Obecné pravidelné služby a SLA, Monitoring a Dohledové služby, HelpDesk služby, Správa serverové výpočetní infrastruktury SUN Sparc, SUN Enterprise, Správa serverové výpočetní infrastruktury IBM x86, Správa serverové výpočetní infrastruktury IBM POWER, Správa serverové výpočetní infrastruktury HPe, Správa prostředí Managementu, SAN a diskových polí, Správa LAN prvků DC, Správa virtualizační platformy VMware, Správa služby MS Active Directory, Správa služby Certifikační autorita, Správa infrastrukturních služeb, Správa databázových serverů pro ORACLE, Správa databázových serverů pro MS SQL, Správa databázových serverů pro INFORMIX, Správa služby MS Exchange Server a Správa MS Windows serverů a Linux serverů.

V rámci přebíracího období musí být jasně specifikovány měřitelné parametry dle katalogového listu, pro zajištění vyhodnocování této služby. Pro zajištění dohledu fungování zálohování bude využita komponenta Veritas NetBackup OpsCenter a pro sběr informací dále aplikace Helpdesk, kde budou evidovány a vyhodnocovány potřebné hodnoty dle katalogového listu.

Tyto měřitelné hodnoty bude obsahovat pravidelný report, který bude uvádět konkrétní naměřené hodnoty a tím i informace o plnění služby a jejího SLA.

Metodický a procesní postup převzetí služeb

Pro zajištění převzetí uvedené služby bude použita projektová metodika PRINCE2® dle které budou zajištěny veškeré náležitosti, jako jsou:

- Celkové naplánování převzetí služby – seznam dílčích kroků, jejich vzájemných vazeb a termínů zahájení a ukončení
- Definice rizik v převzetí služby
- Koordinace třetích stran a optimalizovat potřebné součinnosti při převzetí služby

Převzetí služby bude dále probíhat dle metodiky ITIL, která zajistí převzetí požadovaných služeb dle definovaných standardů. Použitá metodika bude řešit zejména níže uvedené oblasti.

- Definice požadované služby
- Nastavení služby
- Testovací provoz služby
- Validace služby
- Řízení změn
- Měření služby

Při převzetí služeb je nutné zohlednění metodik a politik v prostředí Zadavatele, a to zejména vydaných metodických pokynů a jednotlivých provozních řádů. Konkrétně se jedná o:

- Politika bezpečnosti informací Magistrátu hl. m. Prahy
- Technická bezpečnostní politika správy ICT
- Technická bezpečnostní politika sítí
- Technická bezpečnostní politika konfigurace ICT
- Instrukce pro přístup do oblastí zajištěných PZTS
- Metodický pokyn č. 7/2017–k řízení bezpečnostních událostí a bezpečnostních incidentů
- Metodický pokyn č. 8/2017 - Pravidla užívání informačního systému Magistrátu hl. m. Prahy
- Metodický pokyn č. 2/2018–k systému řízení IT služeb
- Metodický pokyn č. 1/2019 – Provozní řád datového centra DC4
- Metodický pokyn č. 2/2019 – Provozní řád datového centra DC5

Návrh harmonogramu

Detail činnosti	T+2	T+4	T+6	T+8	T+10	T+12
Příprava plánu převzetí						
Předání a seznámení se s dokumentací						

Nastavení oprávnění						
Provedení analýzy prostředí						
Kontrola prostředí zálohování a politik						
Ověření stavu zálohování a kapacit						
Nastavení návazných procesů - monitoring						
Workshop před převzetím služby						
Převzetí služby						

(T=počty dnů)

Požadovaná součinnost zadavatele

- Dodání dokumentace zálohování a veškeré související infrastruktury, seznamu souvisejícího HW a SW, seznamu a obsahu procesů zálohování a procesů navazujících na zálohování
- Nastavení fyzického i elektronického přístupu k dotčeným systémům pro poskytovatele
- Dodání souhrnu požadovaných provozních parametrů zálohování (plán zálohování)
- Nastavení kontaktních a zodpovědných osob do kontaktní matice, a to včetně kontaktů pro komunikaci s dalšími navazujícími službami
- Dodání přístupových oprávnění ke všem příslušným systémům
- Stanovení vzoru pravidelného reportingu

Analýza rizik v dané oblasti

V rámci analýzy a řízení rizik je potřeba postupovat následujícími kroky „Identifikace" -> „Hodnocení" -> „Implementace". Analýza rizik je prováděna dle odhadnuté pravděpodobnosti a dopadu.

Pro převzetí uvedené služby jsme identifikovaly následující rizika:

Riziko	Hodnocení rizika	Návrh nápravného opatření
Nedodržení časového harmonogramu	Střední	Včasné zajištění veškerých potřebných podkladů a součinností pro převzetí služby
Přístup k informacím pro provedení analýzy	Střední	Včasné předání veškerých potřebných informací a přístupů pro provedení analýzy
Nedostatečná nebo žádná dokumentace k provozovaným systémům	Střední	Zajistit podporu Zadavatele pro optimalizaci, stanovení odpovědnosti na straně Zadavatele a zajištění potřebných vstupů
Poškození dat	Střední	Pro minimalizování rizika je nutné mít zajištěny zálohy dohledového systému
Nesoučinnost třetích stran	Střední	Včasné kontaktování třetích stran pro zajištění

		potřebných součinností
Nedostatečné informace o zálohovacím řešení	Nízké	Zajistit podporu objednatele, stanovení odpovědnosti na straně objednatele
Nezajištění fyzického nebo elektronického přístupu k systémům	Nízké	Včasné otevření komunikace o přístupech a všech nutných podmínkách
Nezajištění všech nutných přístupových oprávnění (účtů) k systémům	Nízké	Zajistit včasnou validaci všech účtů a oprávnění nutných pro provedení převzetí i následné poskytování služby
Nesprávné kontakty v komunikační matici	Nízké	Zajistit včasnou validaci všech kontaktů nutných pro provedení převzetí i následné poskytování služby
Chybějící návaznost na ostatní služby a chybějící kontakt pro případ potřeby.	Nízké	Ověřit všechny vazby ostatních služeb na zálohování. Zajistit a validovat kontakty u všech navazujících služeb, které budou v případě potřeby spolupracovat

KL15 – Správa prostředí Integrační platformy

Popis návrhu převzetí služeb

Před převzetím služby je nutné nejdříve stanovit jasný plán převzetí. Tento plán musí obsahovat: Vymezení hlavních kontaktních osob, definice procesů, způsob omezování rizik, definice akceptačních kritérií a harmonogram převzetí služeb.

Následně bude nutné jasně specifikovat procesy v rámci převzetí služeb, a to zejména v oblasti kontroly změn, kontroly sporných skutečností a kontroly rizik v převzetí služby. Dále bude nutné vytvořit komunikační matici pro nastavení komunikačních kanálů v této oblasti pro zajištění informovanosti při přebíracím období. V rámci přebíracího období bude definován popis Implementačních kritérií, procesu testování a akceptace připravenosti na započetí poskytování cílových služeb. Při převzetí služeb bude zohledněn dopady na zaměstnance koncového Zákazníka, dopad na interní procesy a postupy koncového Zákazníka, připravenost vybavení, rozhraní a procesů nutných pro bezproblémové zahájení poskytování cílových služeb, finanční a obchodní dopady zahájení poskytování Cílových služeb.

Před převzetím této služby je nejprve nutné provést analýzu této oblasti. Je nutné zajistit detailní dokumentaci k danému prostředí, které musí obsahovat veškeré náležitosti, dále je nutné zajistit informace o použitých licencí. Je nutné provést kontrolu jednotlivých virtuálních i fyzických serverů kde je aplikace naisntalována. Další důležitý bod celé

architektura prostředí a celé workflow aplikace. Je nutné provést kontrolu jednotlivých komponent API Gateway, API Manager, API Analytika a developerský portál. Dále je nutné prověřit integrované aplikace do samotné IP a jejich procesní funkčnost. Dále je nutné prověření využití XML/SOAP služeb v souladu s definicí centrálních služeb.

Po uvedené analýze musí dojít k vytvoření nových administrátorských přístupů pro možnost správy prostředí a odebrání původních přístupů.

Následně budou převzaté systémy zaneseny do dokumentace, připraven návrh pravidelných zásahů na prostředí, zajištěno monitorování prostředí a nastavení SLA parametrů pro definované služby.

Po těchto krocích dojde k převzetí uvedené služby.

Přístup k řešení dané oblasti

Převzetí uvedené služby bude stanoveno dle standardních využívaných metodik a v závislosti na poskytovaných službách tak, aby nedošlo k omezení poskytovaných služeb a zároveň aby služba byla převzata s veškerými důležitými závislostmi na další poskytované služby a aby nedošlo k omezení těchto služeb během přebíracího období.

Oblast poskytování uvedené služby Správa prostředí Integrační platformy je závislé na obecných a pravidelných službách SLA, Monitoring a Dohledové služby, HelpDesk služby, Správa serverové výpočetní infrastruktury IBM POWER, Správa serverové výpočetní infrastruktury HPe, Správa prostředí Managementu, SAN a diskových polí, Správa LAN prvků DC, Správa virtualizační platformy VMware, Správa služby MS Active Directory, Správa infrastrukturních služeb, Správa databázových serverů pro ORACLE, Správa databázových serverů pro MS SQL, Správa služby MS Exchange Server a Správa MS Windows serverů a Linux serverů.

V rámci přebíracího období musí být jasně specifikovány měřitelné parametry dle katalogového listu, pro zajištění vyhodnocování této služby. Jednotlivé parametry SLA budou vyhodnocovány z dohledového nástroje, který tyto parametry eviduje. Tyto měřitelné hodnoty bude obsahovat pravidelný report, ve kterém budou uvedené hodnoty a tím i informace o plnění uvedené služby.

Metodický a procesní postup převzetí služeb

Pro zajištění převzetí uvedené služby bude použita projektová metodika PRINCE2® dle které budou zajištěny veškeré náležitosti, jako jsou:

- Celkové naplánování převzetí služby – seznam dílčích kroků, jejich vzájemných vazeb a termínů zahájení a ukončení
- Definice rizik v převzetí služby
- Koordinace třetích stran a optimalizovat potřebné součinnosti při převzetí služby

Převzetí služby bude dále probíhat dle metodiky ITIL, která zajistí převzetí požadovaných služeb dle definovaných standardů. Použitá metodika bude řešit zejména níže uvedené oblasti.

- Definice požadované služby
- Nastavení služby

- Testovací provoz služby
- Validace služby
- Řízení změn
- Měření služby

Při převzetí služeb je nutné zohlednění metodik a politik v prostředí Zadavatele, a to zejména vydaných metodických pokynů a jednotlivých provozních řádů. Konkrétně se jedná o:

- Politika bezpečnosti informací Magistrátu hl. m. Prahy
- Technická bezpečnostní politika správy ICT
- Technická bezpečnostní politika sítí
- Technická bezpečnostní politika konfigurace ICT
- Instrukce pro přístup do oblastí zajištěných PZTS
- Metodický pokyn č. 7/2017–k řízení bezpečnostních událostí a bezpečnostních incidentů
- Metodický pokyn č. 8/2017 - Pravidla užívání informačního systému Magistrátu hl. m. Prahy
- Metodický pokyn č. 2/2018–k systému řízení IT služeb
- Metodický pokyn č. 1/2019 – Provozní řád datového centra DC4
- Metodický pokyn č. 2/2019 – Provozní řád datového centra DC5

Návrh harmonogramu

Detail činnosti	T+2	T+4	T+6	T+10	T+12
Příprava plánu převzetí					
Předání a seznámení se s dokumentací					
Nastavení oprávnění					
Provedení analýzy prostředí					
Nastavení návazných procesů - monitoring					
Workshop před převzetím služby					
Převzetí služby					

(T=počty dnů)

Požadovaná součinnost zadavatele

- Nastavení fyzického i elektronického přístupu k dotčeným systémům pro poskytovatele
- Dodání dokumentace zálohování a veškeré související infrastruktury, seznamu souvisejícího HW a SW, seznamu a obsahu procesů zálohování a procesů navazujících na zálohování
- Dodání souhrnu požadovaných provozních parametrů Integrační platforma
- Nastavení kontaktních a zodpovědných osob do kontaktní matice, a to včetně kontaktů pro komunikaci s dalšími navazujícími službami
- Dodání přístupových oprávnění ke všem příslušným systémům
- Stanovení vzoru pravidelného reportingu
- Seznam napojených aplikací
- Zajištění VPN přístupu

Analýza rizik v dané oblasti

V rámci analýzy a řízení rizik je potřeba postupovat následujícími kroky „Identifikace" -> „Hodnocení" -> „Implementace". Analýza rizik je prováděna dle odhadnuté pravděpodobnosti a dopadu.

Pro převzetí uvedené služby jsme identifikovaly následující rizika:

Riziko	Hodnocení rizika	Návrh nápravného opatření
Nedodržení časového harmonogramu	Střední	Včasné zajištění veškerých potřebných podkladů a součinností pro převzetí služby
Nedostatečný přístup k informacím pro provedení analýzy	Střední	Včasné předání veškerých potřebných informací a přístupů pro provedení analýzy, správné nastavení komunikační matice
Nedostatečná nebo žádná dokumentace k systémům	Střední	Zajistit podporu objednatele, stanovení odpovědnosti na straně objednatele a zajištění potřebných vstupů. Detailní validace dokumentace vůči skutečnosti.
Nedostatečný popis síťového propojení systému s ostatní infrastrukturou	Střední	Zdůraznit význam přesné znalosti síťového zapojení (adresy, porty, prostupy, subnety, firewallly) Integrčaní platformy při získávání dokumentace
Nesoučinnost třetích stran	Střední	Včasné kontaktování třetích stran pro zajištění potřebných součinností, stanovení odpovědnosti a rozhodovací pravomoci na straně objednatele
Nezajištění fyzického nebo elektronického přístupu k systémům	Nízké	Včasné otevření komunikace o přístupech a všech nutných podmínkách
Nezajištění všech nutných přístupových oprávnění (účtů) k systémům	Nízké	Zajistit včasnou validaci všech účtů a oprávnění nutných pro provedení převzetí i následné poskytování služby
Nesprávné kontakty v komunikační matici	Nízké	Zajistit včasnou validaci všech kontaktů nutných pro provedení převzetí i

		následné poskytování služby
Chybějící návaznost na ostatní služby a chybějící kontakt pro případ potřeby.	Nízké	Ověřit všechny vazby ostatních služeb na infra Integrační platforma. Zajistit a validovat kontakty u všech navazujících služeb, které budou v případě potřeby spolupracovat
Poškození dat	Střední	Pro minimalizování rizika je nutné mít zajištěny zálohy dohledového systému
Systémy bez podpory	Nízká	Zajištění základní servisní podpory provozovaných systémů

2. <u>Harmonogram plnění</u>

ID	Milník	Termín
1.	Nabytí účinnosti Rámcové dohody	T
2.	Poskytnutí Služeb převzetí	T+ max. 18 dnů
3.	Akceptace Služby převzetí	T+ max. 20 dnů
4.	Poskytnutí služeb katalogových listů	T+ max. 25 dnů

Příloha č. 3

Realizační tým Poskytovatele

Pozice (role)	Identifikační a kontaktní údaje osoby	Dodavatel / člen společnosti dodavatelů / poddodavatel, k němuž osoba patří	Počet obdržených bodů v rámci hodnocení
Projektový manažer	Jaromír Žák Telefon: [redacted]	Dodavatel	[redacted]
Specialista architekt řešení	Ondřej Salák Telefon: [redacted]	Dodavatel	
Specialista řízení IT služeb	Tomáš Myslivec Telefon: [redacted]	Dodavatel	
IT specialista na prostředí Microsoft Exchange Server	Jiří Veličkov Telefon: [redacted]	Dodavatel	
IT specialista na databázové systémy – MS SQL	Josef Medáček Telefon: [redacted]	Dodavatel	
IT specialista na databázové systémy – ORACLE	Tomáš Solař Telefon: [redacted]	Dodavatel	
IT specialista na databázové systémy – INFORMIX	Marek Patočka Telefon: [redacted]	Dodavatel	
IT specialista pro systémy LAN	Jan Půlpán Telefon: [redacted]	Dodavatel	
IT specialista na systémy Firewall CISCO	Michal Dubec Telefon: [redacted]	Dodavatel.	
IT specialista na systémy Firewall – Checkpoint	Lukáš Sosnovec Telefon: [redacted]	Dodavatel	
IT specialista pro serverovou infrastrukturu (Intel servery)	Ondřej Klivan Telefon: [redacted]	Dodavatel	
IT specialista pro serverovou infrastrukturu (Power servery)	Marek Doležal Telefon: [redacted]	Dodavatel	

IT specialista pro infrastrukturu pro ukládání dat HPE 3PAR a sítě SAN	Ladislav Božovský Telefon: [redacted]	Dodavatel	[redacted]
IT specialista pro infrastrukturu pro ukládání dat IBM Storwize a sítě SAN	Petr Bretšnajdr Telefon: [redacted]	Dodavatel	
IT specialista na OS Microsoft Windows Server – Active Directory	Petr Horský Telefon: [redacted]	Dodavatel	
IT specialista na serverové operační systémy OS Linux Red Hat	Tomáš Horáček Telefon: [redacted]	Dodavatel	
IT specialista na serverové virtualizační datacentrové systémy Vmware	Martin Kapl Telefon: [redacted]	Dodavatel	
IT specialista na desktopové virtualizační datacentrové systémy CITRIX	Petr Jeřábek Telefon: [redacted]	Poddodavatel AUTOCONT a.s.	
IT specialista na řešení ochrany poštovních serverů a koncových stanic SYMANTEC	Vladimír Čapek Telefon: [redacted]	Poddodavatel AUTOCONT a.s.	
IT specialista na systémy IP Monitoringu sítí	Petr Borovička Telefon: [redacted]	Dodavatel	
IT specialista na systémy SIEM QRADAR	Karel Goldmann Telefon: [redacted]	Dodavatel	
IT specialista na systémy SIEM – ochrana databází Guardium	Radim Navrátil Telefon: [redacted]	Dodavatel	
IT specialista na systémy DataPower Gateway	Ing. Ondřej Novák Telefon: [redacted]	Dodavatel	
IT specialista na Microsoft Azure a Cloud	Michal Barták Telefon: [redacted]	Dodavatel	

IT specialista integrační platformy	Filip Horák Telefon: [redacted]	Dodavatel	[redacted]

Příloha č. 4

Oprávněné osoby

Za Objednatele:

ve věcech smluvních:

Jméno a příjmení	Mgr. Jiří Károly
Adresa	Praha 1, Nové Město, Jungmannova 35
E-mail	[redacted]
Telefon	[redacted]

ve věcech obchodních:

Jméno a příjmení	Mgr. Jiří Károly
Adresa	Praha 1, Nové Město, Jungmannova 35
E-mail	[redacted]
Telefon	[redacted]

ve věcech technických:

Jméno a příjmení	Bc. Ladislav Tobiáš, MSc, MPA
E-mail	[redacted]
Telefon	[redacted]

Za Poskytovatele:

ve věcech smluvních:

Jméno a příjmení	Václav Novák, MBA
Adresa	U Uranie 18, 17000 Praha 7
E-mail	[redacted]
Telefon	

ve věcech obchodních:

Jméno a příjmení	Ing. Jiří Hamouz
Adresa	U Uranie 18, 17000 Praha 7
E-mail	[redacted]
Telefon	

ve věcech technických:

Jméno a příjmení	Ing. Tomáš Myslivec
Adresa	U Uranie 18, 17000 Praha 7
E-mail	[redacted]
Telefon	

Příloha č. 5

Seznam poddodavatelů

1)

Název:	**AUTOCONT a.s.**
Sídlo:	Hornopolní 3322/34, 702 00 Ostrava
Právní forma:	akciová společnost
Identifikační číslo:	04308697
Rozsah plnění Rámcové dohody:	40 %

Poskytnutí techniků realizačního týmu na pozice:

IT specialista na řešení ochrany poštovních serverů a koncových stanic SYMANTEC (p. Vladimír Čapek)
IT specialista na desktopové virtualizační datacentrové systémy CITRIX (p. Petr Jeřábek)

Plnění následujících částí zakázky

KL04b – Správa serverové výpočetní infrastruktury technologie IBM x86 (DC0,DC1)

KL06 – Správa LAN prvků DC (DC0)

KL08 – Správa služby MS Active Directory (DC0, DC1, DC4, DC5)

KL09 – Správa služby Certifikační autorita (DC0, DC1, DC4, DC5)

KL10 – Správa infrastrukturních služeb (DC0, DC1)

KL11a – Správa databázových serverů Oracle (DC0, DC1)

KL11b – Správa databázových serverů MS SQL (DC0, DC1, DC4, DC5)

KL11c – Správa databázových serverů pro INFORMIX (DC0)

KL12 – Správa služby MS Exchange Server (DC0, DC1, DC4, DC5)

KL13 – Správa MS Windows serverů a Linux serverů (DC0, DC1, DC4, DC5)

a

Plnění technické kvalifikace

1. Poskytnutí významných dodávek a služeb kategorie B (Dodávka HW, SW a služeb v oblasti infrastruktury datových center pro MHM computer a.s. a PODPORA A SPRÁVA ICT INFRASTRUKTURY pro AHOLD Czech Republic, a.s.)

Příloha č. 6

Detailní rozpad Cena za Služby

Tato příloha upravuje jednotkové ceny za poskytování Služeb dle Rámcové dohody:

Cena za poskytování Služeb převzetí dle Rámcové dohody:

Služby převzetí	Cena v Kč bez DPH
Cena za poskytnutí Služeb převzetí *Pozor limitace maximálně 5 % z Celková nabídkové ceny dodavatele*	932.230,-

Jednotkové ceny Služeb specialistů dle Rámcové dohody:

Pozice	Cena v Kč bez DPH za jednotku (člověkoden)
Projektový manažer	12.000,-
Specialista architekt řešení	12.000,-
Specialista řízení IT služeb	10.000,-
IT specialista na prostředí Microsoft Exchange Server	10.000,-
IT specialista pro databázové systémy – Microsoft SQL	9.500,-
IT specialista na databázové systémy – ORACLE	12.000,-
IT specialista na databázové systémy - INFORMIX	9.500,-
IT specialita pro systémy LAN	9.500,-
IT specialista na systémy Firewall CISCO	11.000,-
IT specialista na systémy Firewall – Checkpoint	11.000,-
IT specialista pro serverovou infrastrukturu (Intel servery)	8.500,-
IT specialista pro serverovou infrastrukturu (Power servery)	10.000,-
IT specialista pro infrastrukturu pro ukládání dat HPE 3PAR a sítě SAN	11.000,-

IT specialista pro infrastrukturu pro ukládání dat IBM Storwize a sítě SAN	11.000,-
IT specialista na OS Microsoft Windows Server – Active Directory	9.000,-
IT specialista na serverové operační systémy OS Linux Red Hat	9.000,-
IT specialista na serverové virtualizační datacentrové systémy Vmware	10.000,-
IT specialista na desktopové virtualizační datacentrové systémy CITRIX	10.000,-
IT specialista na řešení ochrany poštovních serverů a koncových stanic SYMANTEC	9.500,-
IT specialista na systémy IP Monitoringu sítí	8.500,-
IT specialista na systémy SIEM – QRADAR	10.000,-
IT specialista na systémy SIEM – ochrana databází Guardium	10.000,-
IT specialista na systémy DataPower Gateway	10.000,-
IT specialista na Microsoft Azure a Cloud	9.500,-
IT specialista integrační platformy	10.000,-

Detailní Rozpis ceny za poskytování Služeb dle katalogových listů vč. dílčího rozpadu ceny:

<table>
<tr><th>Specifikace Katalogového listu</th><th colspan="4">Dílčí rozpad ceny v Kč bez DPH za měsíc poskytování Služeb dle Katalogového listu
(je-li u daného Katalogového list zadavatelem požadován)</th><th>Cena za jeden měsíc poskytování všech Služeb dle Katalogového listu
(v Kč bez DPH)
(Pokud je poskytován rozpad dle předchozího sloupce, jedná se o souhrnnou cenu)</th></tr>
<tr><td>KL01 – Obecné pravidelné služby a SLA</td><td colspan="4"></td><td>64.000,-</td></tr>
<tr><td rowspan="2">KL02 – Monitoring a dohledové služby</td><td colspan="2">DC0 + DC1</td><td colspan="2">DC4 + DC5</td><td rowspan="2">30.000,-</td></tr>
<tr><td colspan="2">15.000,-</td><td colspan="2">15.000,-</td></tr>
<tr><td>KL03 – HelpDesk služby</td><td colspan="4"></td><td>25.000,-</td></tr>
<tr><td rowspan="2">KL04a – Správa serverové výpočetní infrastruktury SUN Sparc, SUN Enterprise</td><td>DC0</td><td>DC1</td><td>DC4</td><td>DC5</td><td rowspan="2">40.000,-</td></tr>
<tr><td>20.000,-</td><td>20.000,-</td><td>Nebude dodavatel naceňovat</td><td>Nebude dodavatel naceňovat</td></tr>
<tr><td>KL04b – Správa</td><td>DC0</td><td>DC1</td><td>DC4</td><td>DC5</td><td>30.000,-</td></tr>
</table>

serverové výpočetní infrastruktury IBM x86	20.000,-	10.000,-	Nebude dodavatel naceňovat	Nebude dodavatel naceňovat	
KL04c – Správa serverové výpočetní infrastruktury IBM power	**DC0**	**DC1**	**DC4**	**DC5**	30.000,-
	20.000,-	Nebude dodavatel naceňovat	Nebude dodavatel naceňovat	10.000,-	
KL04d – Správa serverové výpočetní infrastruktury HPe	**DC0**	**DC1**	**DC4**	**DC5**	65.000,-
	Nebude dodavatel naceňovat	15.000,-	25.000,-	25.000,-	
KL05 – Správa prostředí Managementu, SAN a diskových polí	**DC0**	**DC1**	**DC4**	**DC5**	80.000,-
	20.000,-	20.000,-	20.000,-	20.000,-	
KL06 – Správa LAN prvků DC	**DC0**	**DC1**	**DC4**	**DC5**	30.000,-
	5.000,-	5.000,-	10.000,-	10.000,-	
KL07 – Správa virtualizační platformy VMware	**DC0 + DC1**		**DC4 + DC5**		50.000,-
	20.000,-		30.000,-		
KL08 – Správa služby MS Active Directory					25.000,-
KL09 – Správa služby Certifikační autorita					10.000,-
KL10 – Správa	**DC0 + DC1**		**DC4 + DC5**		35.000,-

infrastrukturních služeb	10.000,-		25.000,-		
KL11a – Správa databázových serverů pro ORACLE	**DC0**	**DC1**	**DC4**	**DC5**	130.000,-
	30.000,-	20.000,-	40.000,-	40.000,-	
KL11b – Správa databázových serverů pro MS SQL	**DC0**	**DC1**	**DC4**	**DC5**	110.000,-
	20.000,-	20.000,-	35.000,-	35.000,-	
KL11c – Správa databázových serverů pro INFORMIX	**DC0**	**DC1**	**DC4**	**DC5**	10.000,-
	10.000,-	Nebude dodavatel naceňovat	Nebude dodavatel naceňovat	Nebude dodavatel naceňovat	
KL12 – Správa služby MS Exchange Server					65.000,-
KL13 – Správa MS Windows serverů a Linux serverů	**DC0 + DC1**		**DC4 + DC5**		110.000,-
	30.000,-		80.000,-		
KL14 – Správa zálohování	**DC0 + DC1**		**DC4 + DC5**		130.000,-
	65.000,-		65.000,-		
KL15 – Správa prostředí Integrační platformy					20.000,-

Cena za poskytování Služeb exitu dle Rámcové dohody:

Služby exitu	Cena v Kč bez DPH
Cena za poskytnutí Služeb exitu *Pozor limitace maximálně 5 %* *z Celková nabídkové ceny dodavatele*	93.223,-

Příloha č. 7

Zadávací dokumentace

(volná příloha Rámcové dohody)

Příloha č. 8

ICT standardy Objednatele

ID	Název standardu
1	SA01 Správa koncových zařízení
2	SB04 Služby datového centra – virtualizace
3	SB05 Pronájem optických vláken a DWDM
4	SB06 Správa Firewall
5	SB07 Správa LAN
6	SB08 SLA Container
7	SB09 Antivir
8	SB10 Správa WAN
9	SB11 Poskytování diskového prostoru
10	SB12 Poskytování výpočetního výkonu (HW)
11	SB13 Identity and access management (IAM)
12	SB14 Správa e-mailových služeb
13	SB15 Internet access
14	SB16 VPN gateway
15	SB17 Poskytování služby ServiceDesk
16	SB18 Poskytování monitoringu infrastruktury a služeb
17	SB19 Poskytování služby Licence management
18	SB20 DNS, DHCP a AD
19	SB21 Správa certifikátu a CA
20	SC01 Generická aplikace
21	MC01 Provoz programového vybavení Celopražského významu
22	MC02 Poskytnutí datového prostoru
23	MC03 Bezpečné úložiště
24	MC04 Poskytování výpočetního výkonu v datovém centru
25	MC05 Poskytování podpůrného programového vybavení

PŘÍLOHA Č. 9

Ujednání o ochraně a zpracování osobních údajů

S ohledem na předmět této Rámcové dohody smluvní strany předpokládají, že Poskytovatel bude zpracovávat osobní údaje uživatelů při poskytování některých Služeb dle této Rámcové dohody (dále jen „**Evidované osoby**"). Toto ujednání obsahuje rovněž ujednání o zpracování osobních údajů dle Nařízení GDPR, mezi Objednatelem jako správcem osobních údajů a Poskytovatelem ve smyslu Rámcové dohody jako zpracovatelem osobních údajů, uvedená níže.

1. OBECNÉ ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ EVIDOVANÝCH OSOB

1.1 Objednatel jako správce osobních údajů pověřuje Poskytovatele jako zpracovatele osobních údajů zpracováváním osobních údajů v rozsahu nezbytném pro plnění Rámcové dohody a výhradně za účelem vyplývajícím z účelu Rámcové dohody.

1.2 Povinnosti Poskytovatele týkající se ochrany osobních údajů se Poskytovatel zavazuje plnit i po zániku účinnosti Rámcové dohody.

1.3 Poskytovatel je povinen postupovat při zpracování osobních údajů v souladu s touto Rámcovou dohodou a Nařízením GDPR, a zpracovávat osobní údaje výlučně pro účel a v rozsahu, ve kterém mu byly předány a při zpracování postupovat jako odborník s řádnou péčí tak, aby neporušil žádné ustanovení Nařízením GDPR, či jiného právního předpisu nebo nezpůsobil skutečnost, která by znamenala porušení Nařízení GDPR, či jiného právního předpisu Objednatelem.

1.4 V případě ukončení této Rámcové dohody je Poskytovatel povinen předat Objednateli protokolárně veškeré hmotné nosiče obsahující osobní údaje a smazat veškeré osobní údaje v elektronické podobě v jeho dispozici, neobdrží-li Poskytovatel od Objednatele písemně jiné pokyny nebo nezavazují-li ho k dalšímu zpracování těchto osobních údajů explicitně vymezená plnění právních povinností. O těchto právních povinnostech je v případě ukončení této Rámcové dohody Poskytovatel povinen Objednatele informovat.

1.5 Poskytovatel je povinen dbát, aby žádná Evidovaná osoba neutrpěla újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a také dbát na ochranu Evidovaných osob před neoprávněným zasahováním do soukromého a osobního života.

1.6 Poskytovatel se zavazuje dodržovat všechny povinnosti, které mu jako zpracovateli osobních údajů vyplývají z nařízení GDPR, jakož i z interních předpisů Objednatele a rozhodnutí či doporučení nebo stanovisek vydaných pro Objednatele příslušným orgánem státní správy, s nimiž byl seznámen, a to včetně rozhodnutí či stanovisek nebo doporučení vydaných v budoucnu.

1.7 Za účelem plnění povinností v souvislosti s ochranou a zpracováním osobních údajů dle Rámcové dohody se Objednatel zavazuje bezodkladně po jejich obdržení poskytovat Poskytovateli jakákoliv rozhodnutí či doporučení nebo stanoviska vydaná příslušným orgánem státní správy.

1.8 Poskytovatel je povinen zajistit, že zpracovávání osobních údajů probíhá v souladu s Nařízením GDPR i v tom smyslu, že v případě, že je podle Nařízení GDPR či jiného příslušného právního předpisu vyžadováno jakékoli oznámení nebo jiný úkon vůči Úřadu pro ochranu osobních údajů či jinému správnímu orgánu, upozorní na tuto skutečnost

Objednatele v dostatečném předstihu a v případě, že tím Objednatel Poskytovatele pověří a zmocní, zajistí provedení těchto úkonů.

1.9 Pokud Poskytovatel zjistí, že Objednatel porušuje povinnosti stanovené Nařízením GDPR, je povinen jej na to neprodleně upozornit.

1.10 V případě, kdy je ze strany Úřadu pro ochranu osobních údajů či jiného správního orgánu provedena kontrola zpracování osobních údajů Poskytovatelem či v případě zahájení správního řízení ze strany Úřadu pro ochranu osobních údajů či jiného správního orgánu ve vztahu k zpracování osobních údajů Poskytovatelem, je Poskytovatel tuto skutečnost povinen okamžitě oznámit Objednateli a poskytnout mu veškeré informace o průběhu a výsledcích této kontroly, resp. průběhu a výsledcích takového procesu, včetně kopií veškeré dokumentace (kontrolní protokol, zpráva o přijatých opatřeních k nápravě, atp.).

1.11 Poskytovatel není oprávněn osobní údaje Evidovaných osob jím zpracovávané či k nimž mu byl umožněn přístup žádným způsobem ukládat, kopírovat, tisknout, opisovat, činit z nich výpisky či opisy či je pozměňovat, pokud toto není nezbytné pro plnění jeho povinností dle této Rámcové dohody.

1.12 Poskytovatel je dále povinen řádně vypořádávat požadavky a nároky vznesené subjekty údajů.

1.13 Poskytovatel je povinen umožnit Objednateli na vyžádání kontrolu dodržování povinností dle této přílohy Rámcové dohody, zejména přístupy do prostor, v nichž jsou osobní údaje uchovávány, předložení seznamu osob s přístupem k osobním údajům či doložení, že veškeré osoby přistupující k osobním údajům splňují požadavky pověřené osoby. Poskytovatel je rovněž povinen umožnit Objednateli přístup do databáze s osobními údaji předáním přístupových údajů, a to vždy jednorázově na základě konkrétní žádosti Objednatele.

2. ROZSAH ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

2.1 Poskytovatel bude zpracovávat osobní údaje uživatelů pouze v rozsahu nezbytném pro poskytování Služeb dle Rámcové dohody a pro výkon práv a povinností Poskytovatele dle Rámcové dohody.

2.2 Zpracování osobních údajů uživatelů je Poskytovatel povinen provádět pouze v následujícím rozsahu nezbytně nutném pro plnění práv a povinností Poskytovatele dle Rámcové dohody:

- jméno a příjmení;
- titul (pokud je tento údaj poskytnut);
- emailová adresa (pokud je tento údaj poskytnut);
- telefonní číslo (pokud je tento údaj poskytnut).

3. ZÁRUKY O TECHNICKÉM A ORGANIZAČNÍM ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ EVIDOVANÝCH OSOB

3.1 Poskytovatel je povinen zabezpečit řádnou technickou a organizační ochranu zpracovávaných osobních údajů způsobem stanoveným v Nařízení GDPR či v jiných právních předpisech.

3.2 Poskytovatel je povinen při zpracování osobních údajů zajistit ochranu osobních údajů minimálně na takové úrovni, aby byly dodrženy veškeré záruky o technickém a organizačním zabezpečení osobních údajů uvedené níže v této příloze Rámcové dohody.

3.3 Poskytovatel se zavazuje přijmout taková opatření, aby nemohlo dojít k neoprávněnému ani nahodilému přístupu k osobním údajům, k jejich úplné ani částečné změně, zničení či ztrátě, neoprávněným přenosům či sdružení s jinými osobními údaji, či k jinému neoprávněnému

zpracování v rozporu se Rámcovou dohodou. Poskytovatel zároveň užije taková opatření, která umožní určit a ověřit, komu byly osobní údaje předány. Tato povinnost platí i po ukončení zpracování osobních údajů.

3.4 Poskytovatel se za účelem ochrany osobních údajů zavazuje zajistit zejména, že:

3.4.1 Přístup k osobním údajům bude umožněn výlučně pověřeným osobám, které budou v pracovněprávním, příkazním či jiném obdobném poměru k Poskytovateli, budou předem prokazatelně seznámeny s povahou osobních údajů a rozsahem a účelem jejich zpracování a budou povinny zachovávat mlčenlivost o všech okolnostech, o nichž se dozví v souvislosti se zpřístupněním osobních údajů a jejich zpracováním a dále budou prokazatelně poučeny o dalších povinnostech, které jsou povinny dodržovat tak, aby nedošlo k porušení Nařízení GDPR či jiných právních předpisů (dále jen „**pověřené osoby**"). Splnění těchto povinností zajistí Poskytovatel vhodným způsobem, zejména vydáním svých vnitřních předpisů, příp. prostřednictvím zvláštních smluvních ujednání. Poskytovatel nesvěří zpracování osobních údajů jakékoliv třetí osobě bez předchozího písemného souhlasu Poskytovatele a vždy vhodným způsobem zajistí, že jeho zaměstnanci a jiné osoby, které budou zpracovávat osobní údaje na základě Rámcové dohody s Poskytovatelem, budou zpracovávat osobní údaje pouze za podmínek a v rozsahu Poskytovatelem stanoveném a odpovídajícím této příloze Rámcové dohody a za podmínek Nařízení GDPR, zejména zajistí zachování mlčenlivosti o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů, a to i pro dobu po skončení zaměstnání nebo příslušných prací pověřených osob.

3.4.2 Při zpracování osobních údajů budou osobní údaje uchovávány výlučně na zabezpečených serverech nebo na zabezpečených nosičích dat a s využitím programového vybavení tak, aby byl vyloučen neoprávněný či nahodilý přístup k osobním údajům ze strany jiných osob, než pověřených zaměstnanců Poskytovatele, jedná-li se o osobní údaje v elektronické podobě.

3.4.3 Při zpracování osobních údajů v jiné, než elektronické podobě budou osobní údaje uchovány v objektech a místnostech s náležitou úrovní zabezpečení, do kterých budou mít přístup výlučně pověřené osoby, a bude vedena řádná evidence o pohybu dokumentů obsahujících osobní údaje.

3.4.4 Přístup k osobním údajům bude pověřeným osobám umožněn výlučně pro účely zpracování osobních údajů v rozsahu a za účelem stanoveným touto Rámcovou dohodou. Přístup bude umožněn na základě přístupových kódů či hesel, tak aby byl každý přístup zaznamenán; osobní údaje budou pravidelně zálohovány.

3.4.5 Poskytovatel zajistí dálkový přenos osobních údajů, buď pouze prostřednictvím veřejně nepřístupné sítě, nebo prostřednictvím zabezpečeného přenosu po veřejných sítích.

3.5 Poskytovatel se zavazuje na písemnou a odůvodněnou žádost Objednatele přijmout v přiměřené lhůtě další záruky za účelem technického a organizačního zabezpečení osobních údajů, zejména přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům.

3.6 Poskytovatel se zavazuje zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu s Nařízením GDPR a jinými právními předpisy, přičemž zajišťuje, kontroluje a odpovídá zejména za:

3.6.1 plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům,

3.6.2 zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování,

3.6.3 zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje a

3.6.4 opatření, která umožní určit a ověřit, komu byly osobní údaje zpřístupněny nebo předány.

3.7 V případě zjištění porušení záruk dle této přílohy Rámcové dohody je Poskytovatel povinen zajistit stav odpovídající zárukám neprodleně poté, co zjistí, že záruky porušuje, nejpozději však do tří (3) pracovních dnů poté, co je k tomu Objednatelem vyzván.

3.8 V oblasti automatizovaného zpracování osobních údajů je Poskytovatel v rámci opatření podle předchozích odstavců povinen také:

3.8.1 zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze pověřené osoby,

3.8.2 zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby,

3.8.3 pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány, a zabránit neoprávněnému přístupu k datovým nosičům.

4. DOBA ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ A ODPOVĚDNOST POSKYTOVATELE

4.1 Poskytovatel bude osobní údaje uživatelů zpracovávat podle této přílohy Rámcové dohody po dobu poskytování Služeb dle Rámcové dohody.

4.2 Po uplynutí doby zpracování osobních údajů podle odstavce 4.1 této Přílohy Rámcové dohody mohou být osobní údaje Evidovaných osob Poskytovatelem zpracovávány pouze v nezbytném rozsahu a výhradně pro plnění právních povinností, které na Poskytovatele v souvislosti s ochranou osobních údajů dopadají, nebo za účelem ochrany práv a právem chráněných zájmů Objednatele a Poskytovatele, nebo jiné dotčené osoby, a to nejdéle do konce pátého kalendářního roku následujícího po roce, v němž skončí doba zpracování osobních údajů podle odstavce 4.1 této Přílohy Rámcové dohody. Poskytovatel jednotlivé osobní údaje zlikviduje, jakmile pomine účel, pro který byly osobní údaje zpracovávány.

4.3 Poskytovatel odpovídá subjektům údajů za škodu a nemajetkovou újmu způsobenou porušením povinnosti Poskytovatele v souvislosti se zpracováním osobních údajů. Poskytovatel dále odpovídá Objednateli za škodu a nemajetkovou újmu způsobenou vznikem povinnosti Objednatele hradit v souvislosti se zpracováním osobních údajů na základě Rámcové dohody nebo v souvislosti s ní jakoukoli náhradu škody a nemajetkové újmy subjektu osobních údajů nebo pokutu Úřadu pro ochranu osobních údajů či jinému správnímu orgánu v důsledku porušení povinností uložených Poskytovateli zákonem nebo Rámcovou dohodou.

4.4 Poskytovatel se zavazuje trvale vyhodnocovat plnění zákonných povinností souvisejících se zpracováním osobních údajů při provozu infrastruktury a průběžně navrhovat veškerá

nezbytná opatření a změny ujednání o zpracování osobních údajů, které zajistí řádné plnění veškerých povinností Poskytovatele souvisejících s ochranou osobních údajů.

Příloha č. 10

Požadavky na zajištění kybernetické bezpečnosti (Kybernetické požadavky)

Za účelem povinností stanovených Objednateli jakožto povinné osobě vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), je Poskytovatel povinen nad rámec povinností stanovených Rámcovou dohodou plnit níže uvedené povinnosti zejm. součinnostního a bezpečnostního charakteru dle této **Přílohy č. 10** Rámcové dohody.

Poskytovatel je povinen plnit relevantní povinnosti v rozsahu a způsobem, aby byl naplněn účel právní úpravy oblasti bezpečnostních opatření, kybernetických bezpečnostních incidentů, reaktivních opatření, náležitostí podání v oblasti kybernetické bezpečnosti a likvidaci dat ve vztahu k povinnostem, které tato právní úprava stanovuje Objednateli jakožto povinné osobě dle předpisů z oblasti kybernetické bezpečnosti, a to i v případě změny příslušné právní úpravy. V takovém případě je Objednatel oprávněn požadovat od Poskytovatele přiměřenou součinnost i nad rámec povinností stanovených v této **Příloze č. 10** Rámcové dohody, avšak vždy pouze za účelem zajištění plnění povinnosti Poskytovatele z oblasti kybernetické bezpečnosti ve smyslu shora uvedeného.

Čl. 1 Systém řízení bezpečnosti informací

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 3 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) (dále jen „**VKB**"), které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:
    a. Prosadit bezpečnostní zásady a procesy, které budou pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně Poskytovatele při poskytování předmětu plnění.
    b. Na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění, monitorovat je, vyhodnocovat jejich účinnost.
    c. Vést záznamy o vytváření a zpracování dat a informací v rozsahu poskytovaného předmětu plnění, zaznamenávat veškeré podstatné okolnosti související se zajištěním bezpečnosti těchto dat a informací a na vyžádání tyto záznamy Objednateli zpřístupnit.
    d. Stanovit a udržovat aktuální bezpečnostní politiku, která bude pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně Poskytovatele při poskytování předmětu plnění. Bezpečnostní politika musí obsahovat hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací.
    e. Stanovit a udržovat aktuální opatření bezpečnosti ve formě procesů a technologií, které zajišťují naplnění bezpečnostní politiky.

Čl. 2 Řízení aktiv

2. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 4 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:

a. Stanovit a udržovat rozsah a seznam aktiv využívaných pro plnění této Rámcové dohody (aktivy se rozumí např. data a informace k předmětu plnění dle této Rámcové dohody, systémy ICT, moduly, HW prvky - infrastruktura hlasové a datové komunikace, aplikace, databáze, servery, úložiště, koncová zařízení – pracovní stanice typu osobní počítač nebo notebook, mobilní koncová zařízení – přenosná zařízení typu telefon, tablet, notebook, netbook, PDA, apod.), a tato aktiva strukturovaně popsat a Objednateli předložit do 30 dnů od podpisu této Rámcové dohody a následně na vyžádání, a to po celou dobu trvání Rámcové dohody a do 2 let po jejím ukončení.

Čl. 3 Řízení rizik

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 5 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:
    a. Řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění.
    b. V minimálním intervalu 1x ročně vytvořit a předložit Zprávu o řízení kybernetických rizik, která bude minimálně pokrývat:
        i. Vyhodnocení stavu kybernetické bezpečnosti za hodnocený rok
        ii. Identifikaci a hodnocení rizik s vazbou na předmět plnění
        iii. Realizovaná bezpečnostní opatření
        iv. Nepokrytá bezpečnostní rizika a návrh opatření
        v. Vyhodnocení bezpečnostních událostí a incidentů
        vi. Aktuální stav souladu Poskytovatele s těmito Kybernetickými požadavky

Čl. 4 Organizační bezpečnost

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 6 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:
    a. Jmenovat nejpozději do 5 dnů po uzavření této Rámcové dohody odpovědnou kontaktní osobu pro potřeby zajištění plnění těchto Kybernetických požadavků a související komunikaci mezi Smluvními stranami (dále také jen „**Kontaktní osoba**"). Kontaktní osobu sdělí Poskytovatel písemně Objednateli v téže lhůtě. Objednatel stanovuje, že určení Kontaktní osoby pro bezpečnost na straně Poskytovatele nemá dopad na ustanovení článku 16.1.1 a 16.1.3 Rámcové dohody týkající se odpovědných osob ve věcech smluvních a technických.
    b. Využívat pro poskytování předmětu plnění pouze oprávněných osob, které byly řádně seznámeny příslušnými ustanoveními interních řídících aktů Objednatele a mají ověřenou kvalifikaci, znalosti a zkušenosti k řádnému poskytování předmětu plnění.

Čl. 5 Řízení dodavatelů

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 8 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:

a. Využívá-li při poskytování předmětu plnění poddodavatele, zajistit adekvátní dodržování Kybernetických požadavků rovněž ve smluvních vztazích se svými poddodavateli, přičemž tuto skutečnost se Poskytovatel zavazuje doložit Objednateli do 10 dnů od Potvrzení objednávky, na jejímž plnění se budou poddodavatelé podílet v případě Služeb specialistů nebo do 10 dnů od počátku poskytování jiných služeb, písemným prohlášením o dodržování Kybernetických požadavků u svých poddodavatelů.

b. Pokud při poskytování předmětu plnění dochází ke zpracování osobních údajů, zajistit nad rámec čl. 17 a **Přílohy č. 9** Rámcové dohody uzavření samostatných smluv (tj. smluv se svými poddodavateli, zaměstnanci a případnými dalšími osobami podílejícími se na poskytování plnění z této Rámcové dohody) ve smyslu příslušných ustanovení Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

Čl. 6 Bezpečnost lidských zdrojů

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 9 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:

    a. Zajistit, aby Kontaktní osoba nejpozději do 30 dnů od uzavření Rámcové dohody potvrdila písemně Objednateli, že všechny osoby podílející se na poskytování předmětu plnění za stranu Poskytovatel byly prokazatelně seznámeny s těmito Kybernetickými požadavky a příslušnými ustanoveními interních řídících aktů Objednatele.

    b. Dodržovat příslušná ustanovení interních řídících aktů Objednatele v rozsahu, v jakém byl s těmito akty seznámen. Za prokazatelné seznámení se považuje školení pracovníků Poskytovatel zajištěné Objednatelem, protokolární či elektronické předání příslušné dokumentace nebo Objednatelem zajištěný přístup na sdílené úložiště obsahující příslušné interní akty řízení.

    c. V případě, že je součástí předmětu plnění služba dohledu nad předmětem plnění, definovat a naplnit role a odpovědnosti pro monitoring sítě a zařízení v rozsahu předmětu plnění.

    d. Zajistit, aby osoby podílející se na poskytování plnění Objednateli v prostředí nebo s prostředky Objednatele, a to i tehdy, pokud jsou prostředky Objednatele používány mimo jeho prostředí:

        i. Pro uložení a sdíleni dat a informací Objednatele využívaly pouze k tomu schválené prostředky (aktiva);

        ii. Neukládaly ani nesdílely data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno Objednatele;

        iii. Nestahovaly, nesdílely, neukládaly, nearchivovaly ani neinstalovaly datové a spustitelné soubory v rozporu s licenčními podmínkami nebo autorským zákonem;

        iv. Nenavštěvovaly internetové stránky s eticky nevhodným obsahem;

        v. Nerealizovaly pokusy o neautorizovaný přístup ke zdrojům Objednatele ani ke zdrojům jiných subjektů;

        vi. Nerealizovaly pokusy o neoprávněnou modifikaci ani jiné neoprávněné zásahy do prostředků Objednatele, a to ani v případě, kdy jim byl prostředek Objednatele svěřen do správy;

vii. Nepodílely se s prostředky Objednatele na šíření spamu ani škodlivého softwaru.

2. Dodavatel si je vědom, že součástí podmínek pro získání přístupu ke zdrojům a aktivům Objednatele je na straně Objednatele zpracování osobních údajů pracovníků Poskytovatele, kteří se podílejí na zajištění předmětu plnění. Pokud nebude Objednateli umožněno osobní údaje dotčených pracovníků Poskytovatele v rámci plnění Rámcové dohody zpracovat, nebude těmto pracovníkům umožněn žádný přístup ke zdrojům Objednatele.

Čl. 7 Řízení provozu a komunikací

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 10 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:

    a. Zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění.

    b. Na vyžádání poskytnout Objednateli přehled, report, či jinou adekvátní informaci o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře.

    c. Zajistit, že pro poskytování předmětu plnění budou využívány pouze aplikace a technologie, které jsou v souladu s platnou českou a evropskou legislativou, především s ohledem na licenční podmínky a autorský zákon.

Čl. 8 Řízení změn

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 11 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:

    a. Přiměřeně reagovat na změny na straně Objednatele a upravit na své straně technická a organizační opatření tak, aby odpovídala novému stavu po provedení změny.

    b. Aktivně spolupracovat při testování významné změny.

Čl. 9 Řízení přístupu

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 12 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:

    a. Přidělovat oprávnění svým jednotlivým pracovníkům ve smyslu oprávnění k výkonu činností tak, aby byla minimalizována rizika nežádoucího přístupu k aktivům Objednatele.

    b. Zajistit, aby udělený přístup nebyl sdílen více osobami za stranu Poskytovatele, pokud sdílený přístup nevyžaduje využívaná technologie. V takovém případě musí Poskytovatel vést evidenci využívání sdílených přístupů a tuto na vyžádání předložit Objednateli kdykoli v průběhu trvání účinnosti této Rámcové dohody a 2 roky po ukončení její platnosti.

    c. Stanovit v požadavku na přístup rozsah dat/informací, služby, účelu, pro které je přístup k systému ICT Objednatele požadován a časový údaj o délce platnosti přístupu (např.: na dobu neurčitou / 1 rok / 1 měsíc / 1 den).

d. Zajistit, aby osoby podílející se na poskytování předmětu plnění a mající přístup k informačním aktivům Objednatele chránily autentizační prostředky a údaje a nikdy neposkytovaly neautorizovaný přístup dalším osobám.

e. Průběžně kontrolovat a vyhodnocovat oprávněnost a potřebu přístupu, jak fyzického, tak i logického, u všech osob na straně Poskytovatele, které přistupují do prostředí Objednatele.

2. Poskytovatel bere na vědomí, že přístup k systému ICT je možné povolit pouze fyzické identitě zaměstnance Poskytovatele / poddodavatele Poskytovatele, a to na základě požadavku Poskytovatele na přístup.

3. Poskytovatel bere na vědomí, že přidělení oprávnění zaměstnanci Poskytovatele musí být řízeno principem nezbytného minima a není nárokové.

4. Poskytovatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele (osoby za stranu Poskytovatele) může být příslušný účet zablokován a řešen jako bezpečnostní incident a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům Objednatele).

Čl. 10 Akvizice, vývoj a údržba

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 13 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:

   a. Zajistit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, které jsou předmětem plnění.

   b. Předat Objednateli dokumentaci předmětu plnění minimálně v následujícím rozsahu:

      i. dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů,

      ii. dokumentaci obsahující popis autorizačního konceptu a oprávnění,

      iii. dokumentaci obsahující instalační a konfigurační postupy.

2. V případě, že předmět plnění zahrnuje vývoj softwaru, zavazuje se Poskytovatel:

   a. Dodržovat a implementovat nejlepší praktiky pro bezpečný vývoj softwaru definované na základě smluvního vztahu.

   b. Na vyžádání umožnit Objednateli provedení auditu prováděného nebo provedeného plnění, předložit objednateli vyvíjený kód SW a výstupy z provedeného codereview (automatizovaně prostřednictvím bezpečnostního nástroje i manuálně), po jeho dokončení, pokud není v této Rámcové dohodě stanoveno jinak, a to zejména za účelem ověření skutečnosti, zda Poskytovatel postupuje či postupoval při poskytování plnění v souladu se Rámcovou dohodou a těmito Kybernetickými požadavky.

   c. Poskytovat Objednateli v termínech stanovených Objednatelem, resp. bez zbytečného odkladu požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje softwaru či kdykoli po jeho předání.

   d. Zajistit, že plnění bude obsahovat jen ty součásti, které jsou objektivně potřebné pro řádné provozování softwaru a/nebo které jsou specifikovány výslovně ve Rámcové dohodě (zejména, že software nebude obsahovat žádné nepotřebné komponenty, žádné programové vzorky apod.).

e. Pokud je součástí plnění i instalace operačního systému případně softwaru třetích stran, zajistit v průběhu jeho instalace, že budou použity předepsané verze těchto produktů kompatibilní a funkční v prostředí Objednatele.

f. Zajistit bezpečnost testovacího prostředí u Poskytovatele a ochranu poskytnutých testovacích dat Objednatelem.

g. Zajistit, že do produkčního prostředí Objednatele bude dodán jen předmětem Rámcové dohody specifikovaný kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování předmětu plnění.

h. Zajistit, že v rámci poskytovaného plnění bude dodávaný software

   i. v souladu s bezpečnostními politikami a standardy Objednatele

   ii. otestován na soulad s bezpečnostními politikami Objednatele (platí pro Poskytovatele, pokud byl s takovými bezpečnostními politikami seznámen)

i. Instalovat software pouze na základě Objednatelem předem schválených migračních postupů.

j. Nevyvíjet, nekompilovat a nešířit v prostředí Objednatele programový kód, který má za cíl nelegální ovládnutí, narušení dostupnosti, důvěrnosti nebo integrity nebo neautorizované či nelegální získání dat a informací.

Čl. 11 Zvládání kybernetických bezpečnostních událostí a incidentů

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 14 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:

   a. Stanovit a popsat na své straně činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání bezpečnostních incidentů.

   b. Bez zbytečného odkladu hlásit Objednateli všechny bezpečnostní události a incidenty s potenciálním negativním dopadem na Objednatele, a to stanoveným komunikačním kanálem nebo prostřednictvím Kontaktní osoby.

   c. Vyhodnocovat informace o bezpečnostních incidentech a uchovávat je pro budoucí použití s ohledem na požadavky platné české a evropské legislativy.

   d. V případě vzniku bezpečnostní události a následného zvládání a vyhodnocování bezpečnostního incidentu a/nebo v případě podezření na bezpečnostní incident poskytnout Objednateli aktivní součinnost a relevantní informace o podezřelém zařízení či osobě na straně Poskytovatele.

   e. Bez zbytečného odkladu a po dohodě s Objednatelem realizovat opatření požadovaná Objednatelem v dohodnutých termínech ke snížení dopadu bezpečnostního incidentu nebo zamezení pokračování incidentu.

   f. Spolupracovat při analýze příčin bezpečnostního incidentu a navrhnout opatření s cílem zamezit jeho opakování v případě, že Poskytovatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

2. Poskytovatel bere na vědomí, že postup zvládání bezpečnostního incidentu či jiný důsledek porušení Kybernetických požadavků, jehož příčina je na straně Poskytovatele, nebude posuzován jako okolnost vylučující odpovědnost Poskytovatele za prodlení s řádným a včasným plněním předmětu Rámcové dohody a nebude důvodem k jakékoli náhradě případné újmy Poskytovateli či jiné osobě ze strany

Objednatele. Ostatní ustanovení ohledně odpovědnosti Poskytovatele za prodlení obsažená ve Rámcové dohodě nejsou tímto ustanovením dotčena.

Čl. 12 Řízení kontinuity činností

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 15 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:
    a. Zajistit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování předmětu plnění.
    b. Pravidelně kontrolovat a testovat, že je schopen kontinuitu aktiv zajistit dle sjednané úrovně služeb.

Čl. 13 Kontrola a audit

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 8 a § 16 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění poskytnout adekvátní součinnost při výkonu kontroly Objednatele ze strany Úřadu dle § 23 ZKB.

Čl. 14 Fyzická bezpečnost

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 17 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:
    a. Dodržovat provozní řády budov (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny aktiva systémů ICT, anebo datové nosiče.
    b. V rozsahu předmětu plnění zajistit fyzické zabezpečení, zejména označení, uchování a likvidaci, instalačních, záložních nebo archivních médií a dokumentace v souladu s klasifikací aktiv Objednatele, pokud s ní byl Poskytovatel seznámen.

Čl. 15 Bezpečnostní nástroje

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 18 až § 27 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:
    a. Realizovat bezpečnostní opatření pro odstranění nebo blokování síťového spojení/síťových spojení, které/která neodpovídají požadavkům na ochranu integrity komunikační sítě.
    b. Realizovat přístup z mobilního zařízení do prostředí Objednatele pouze prostřednictvím zabezpečeného připojení virtuální privátní sítě (VPN) nebo zvolit adekvátní technické opatření.
    c. Připojovat do prostředí Objednatele pouze ta síťová zařízení (switch, přístupový bod wifi, router, hub apod.), která prošla schvalovacím procesem a jejich připojení bylo schváleno oprávněnou osobu ve věcech technických na straně Objednatele určenou v této Rámcové dohodě.

d. Bez zbytečného odkladu deaktivovat všechna nevyužívaná zakončení sítě anebo nepoužívané porty aktivního síťového prvku, který je v rozsahu předmětu plnění a je ve správě Poskytovatele.

e. Na aktiva Objednatele neinstalovat a nepoužívat v prostředí Objednatele tyto typy nástrojů, pokud nejsou součástí předmětu plnění:

   i. Keylogger – software nebo hardware, který neautorizovaně zaznamenává stisky kláves s cílem narušit důvěrnost zadávaných dat a informací.

   ii. Sniffer – software nebo hardware umožňující odposlouchávání síťového provozu.

   iii. Analyzátor zranitelností (scanner zranitelností) – softwarový nebo hardwarový nástroj umožňující vyhledávání zranitelností systémů ICT, detekování dostupných síťových služeb a portů, běžících procesů, běžících aplikací a jejich verzí apod.

   iv. Backdoor – skrytý softwarový nebo hardwarový nástroj, který umožňuje obejití schválených autentizačních procedur, instalovaný s cílem budoucího snadnějšího a neautorizovaného přístupu do systému ICT.

   v. Malware a jiný škodlivý software, který narušuje, obchází či jinak omezuje bezpečnostní opatření v prostředí Objednatele.

f. Připojovat do prostředí Objednatele pouze zařízení ICT, která jsou chráněna proti malware a jinému škodlivému softwaru, pokud to jejich technologie umožňuje.

g. Průběžně zaznamenávat a uchovávat data o provozu zařízení ICT (provozní a lokalizační údaje) v rozsahu předmětu plnění a v souladu s požadavky platné české a evropské legislativy.

h. Na vyžádání poskytnout Objednateli report obsahující výsledky monitorování veškerých uživatelských a administrátorských aktivit a jiných událostí v rozsahu předmětu plnění, a to po celou dobu trvání Rámcové dohody a do 2 let po jejím ukončení.

i. Zajistit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění a ochranu získaných informací před jejich neoprávněným čtením nebo změnou.

j. Pro on-line transakce realizované prostřednictvím webových technologií implementovat TLS/SSL certifikáty s cílem zajistit jejich důvěrnost, integritu a identitu komunikujících protistran.

k. Veškeré neveřejné informace poskytnuté Objednatelem chránit vhodným šifrováním a proti neautorizovanému přístupu, a to zejména na mobilních zařízeních.

2. Poskytovatel bere na vědomí, že v případě, kdy technické spojení Objednatele s Poskytovatelem narušuje chod služeb Objednatele, může být toto spojení ihned ukončeno bez předchozího upozornění, pokud tato Rámcová dohoda nestanoví jinak.

3. Poskytovatel bere na vědomí, že veškeré aktivity Poskytovatele a jeho plnění realizované v prostředí Objednatele jsou monitorovány a vyhodnocovány v rozsahu předměty plnění a v souladu s interními dokumenty Objednatele, se kterými byl Poskytovatel seznámen.