**Specifikace předmětu veřejné zakázky**

1. **Aktuální technický stav**
   1. **Hardware**

* Počet fyzických serverů 6ks
* Z toho 2ks serverů zajišťující virtualizaci
* 40x NTB a 104x PC
* Firewally
* Planet CS-2000 2x
* Planet CS-950 2x
* Zálohovací mechanika
* LTO6 2x
  1. **Software**
* Oracle
* Verze 11g
* Verze 12c
* Zálohovací systém DataProtector
* Virtualizace XEN
* BorderManager
* Windows Server 2016 Standard 16 Core CZ
* Windows Exchange 2016

1. **Obecné podmínky komplexní správy IT infrastruktury**

Není-li uvedeno jinak, platí pro komplexní správu IT infrastruktury objednatele tyto podmínky:

* 1. **Lidské zdroje**

Objednatel požaduje pro zajištění komplexní správy IT infrastruktury vždy mít pouze jeden, dlouhodobý primární technický kontakt na pracovníka ze strany dodavatele.

Všem pracovníkům poskytovatele, kteří se budou pohybovat v prostorách objednatele, bude přiřazena identifikační karta, kterou jsou povinni nosit na viditelném místě oděvu vždy, když se budou nacházet v prostorách objednatele.

* 1. **Hot-line služba**

Objednatel od poskytovatele požaduje zajištění dostupnosti hot-line služby v režimu standardní pracovní doby objednatele.

* 1. **SLA podmínky**

Pro potřeby členění provozních problémů jsou definovány 3 Priority, přičemž zařazení provozního problému do jedné z Priorit určuje objednatel:

* Priorita A = provozní problémy znemožňující užívání hardware, software, systémy
* Priorita B = provozní problémy omezující užívání hardware, software, systémy
* Priorita C = provozní problémy, které komplikují postupy při práci s hardware, software, systémem

Komplexní přehled SLA podmínek:



V průběhu řešení provozního problému je pověřený pracovník objednatele oprávněn změnit klasifikaci Priority provozního problému. Změna klasifikace Priority provozního problému se stává účinnou oznámením poskytovateli. Změnou klasifikace se na provozní problém vztahují SLA podmínky dle nové Priority, přičemž výchozím časem pro Vyřešení problému je:

* V případě změny klasifikace Priority na vyšší (tj. z C na B, z C na A, z B na A), čas, kdy došlo ke změně klasifikace Priority
* V případě změny klasifikace Priority na nižší (tj. z A na B, z A na C, z B na C), čas nahlášení provozního problému, nikoli čas změny klasifikace Priority

Reakční dobou se rozumí lhůta, která začíná plynout časem nahlášení provozního problému poskytovateli, do doby než poskytovatel prokazatelně zahájí práce, směřující k vyřešení provozního problému či zajištění náhradního provozu, přičemž přijetí požadavku na vyřešení problému není považováno za zahájení prací.

Do počítání lhůt dle SLA podmínek není započítána doba:

* potřebná k realizaci činností třetích stran, na něž se nevztahují uvedené SLA podmínky
* činnosti, jejichž časová náročnost je limitována použitými technologiemi

Jedná se například o následující:

* opravy HW na základě záručních podmínek, či rozšířených garancí výrobce
* opravy či změny SW ze strany dodavatele / výrobce
* obnovu dat ze zálohy, jejíž časová náročnost je dána použitou technologií zálohování a objemem dat

* 1. **1st level support**

Podpora funkčnosti (1st level support) spočívá v řešení provozních problémů a podpory všech uživatelů objednatele s cílem minimalizovat výpadky systému či nefunkčnost jednotlivých částí systému.

Poskytovatel bude zajišťovat pravidelnou fyzickou přítomnost technického pracovníka v prostorách určených objednatelem k poskytování podpory 1x týdně.

V oblasti poskytování podpory je uchazeč povinen zajistit zastupitelnost svých pracovníků tak, aby pracovníci aktuálně se nacházející u zadavatele mohli vždy reagovat na požadavky zadavatele, dle stanovených reakčních dob.

V rámci služby řešení provozních problémů je nutné zajistit podmínky SLA definované v článku SLA podmínky a zajistit zastupitelnost osob řešících jednotlivé požadavky.

V rámci podpory funkčnosti budou prováděny následující činnosti:

* Poskytování hotline a zajištění dostupnosti osob s dostatečnou znalostí pro řešení provozních problémů
* Řešení veškerých provozních problémů – tj. zahájení prací směřujících k odstranění a vyřešení provozního problému dle SLA, aktivní komunikaci s objednatelem, směřující k vyřešení provozního problému
* Kontrola všech spravovaných systémů dle potřeby, minimálně však jednou týdně
* O každé kontrole bude provedený záznam v technické dokumentaci serverů

1. **Obsah a podmínky poskytované služby „komplexní správy IT infrastruktury“**
   1. **Správa a podpora IT infrastruktury**
      1. **Požadavky na správu serverů**

* Detailní popis a specifikace požadovaných služeb:
* do 4 měsíců od podpisu smlouvy zavedení automatického on-line monitoringu serverových operačních systémů a hardware. Cílem monitoringu je online sledování stavu kritických služeb, operačních systémů a hardwaru (HDD, CPU, FAN,…) s následným zasláním alertu formou SMS a e-mailu o vzniku provozního problému. Monitoring taktéž musí splňovat možnost reportingu sledovaných parametrů. Na základě zjištěných údajů Poskytovatel doporučí a zrealizuje případné obměny nebo upgrade operačních systémů a hardware a do 10 pracovních dnů zajistí odstranění chyb
* na nově pořízené fyzické i virtuální servery zajišťovat do 10 pracovních dní instalace operačních systémů, serverových služeb a aplikací
* po vydání nových informací týkajících se SW patchů, bezpečnostních updatů a nových funkcionalit, do 10 pracovních dnů provést otestování těchto změn, výsledek do 2 pracovních dnů zaznamenat do dokumentace incidentů a v případě ověření bezproblémovosti, tyto updaty do dalších 10 dnů aplikovat na všechny systémy Objednatele
* správa provozovaného komerčního software
* minimálně 2x měsíčně kontrolovat konfiguraci virtualizačního prostředí, operačních systémů a síťových služeb a provádět v ní změny podle aktuálního vývoje poznatků z bezpečnostního a výkonového hlediska. O každé změně provést záznam v technické dokumentaci serverových systémů
* zajišťovat 1x týdně kontrolu záznamů o chybách virtualizačního prostředí, operačních systémů, serverových služeb a hardware, aplikací a následně do 10 pracovních dní realizovat opatření k eliminaci výskytu chyb
* dle SLA podmínek zajišťovat řešení provozních problémů virtualizačního prostředí, operačních systémů, serverových služeb, aplikací a hardware
* realizovat požadavky Objednatele
* provádět zálohování
* vedení technické dokumentace k systému
* vedení dokumentace incidentů
  + 1. **Požadavky na správu e-mailových a komunikačních systémů**

Detailní popis a specifikace požadovaných služeb:

* zajišťovat do 10 pracovních dnů instalace mailových a komunikačních systémů na nově pořízené servery
* po vydání nových informací týkajících se SW patchů, bezpečnostních updatů a nových funkcionalit, do 10 pracovních dnů provést otestování těchto změn, výsledek do 2 pracovních dnů zaznamenat do dokumentace a v případě ověření bezproblémovosti, tyto updaty do dalších 10 pracovních dnů aplikovat na všechny systémy Objednatele
* minimálně 2x měsíčně kontrolovat konfiguraci e-mailových a komunikačních systémů a provádět v ní změny podle aktuálního vývoje poznatků z bezpečnostního a výkonového hlediska. O každé změně provést záznam v dokumentaci incidentů o e-mailových a komunikačních systémech
* zajišťovat 2x měsíčně kontrolu záznamů o chybách mailových a komunikačních systémů a následně do 10 dnů realizovat opatření k odstranění nalezených chyb
* dle SLA podmínek zajišťovat řešení provozních problémů mailových a komunikačních systémů
* realizovat požadavky Objednatele
* zajistit spolehlivou zálohu dat
* vedení technické dokumentace k systému
* vedení dokumentace incidentů
  + 1. **Požadavky na správu databází**

Detailní popis a specifikace požadovaných služeb:

* po vydání nových informací týkajících se SW patchů, bezpečnostních updatů a nových funkcionalit, do 10 pracovních dnů provést otestování těchto změn, výsledek do 2 pracovních dnů zaznamenat do dokumentace a v případě ověření bezproblémovosti, tyto updaty do dalších 10 dnů aplikovat na databáze Objednatele
* minimálně 2x měsíčně zkontrolovat konfiguraci databází a provést změny podle aktuálního vývoje poznatků z bezpečnostního a výkonového hlediska. O každé změně provést záznam v technické dokumentaci serverů
* zajišťovat 2x měsíčně kontrolu záznamů o chybách databází, aplikací a následně do 10 pracovních dní realizovat opatření k eliminaci výskytu chyb
* dle SLA podmínek zajišťovat řešení provozních problémů databází,
* realizovat požadavky Objednatele
* zajistit spolehlivou zálohu dat
* spravovat přístupové údaje k databázím. Správou se rozumí vytváření a mazání oprávnění a rolí pro databáze. Změna přístupových údajů k databázím je možná pouze po úspěšném absolvování schvalovacího procesu. Změnu přístupových údajů může vždy schválit pouze odpovědná osoba ze strany IT Objednatele
* vedení technické dokumentace k systému
* vedení dokumentace incidentů
  + 1. **Požadavky na správu síťových služeb**
* Detailní popis a specifikace všeobecných požadovaných služeb:
* po vydání nových informací týkajících se SW patchů, bezpečnostních updatů a nových funkcionalit, do 10 pracovních dnů provést otestování těchto změn, výsledek do 2 pracovních dnů zaznamenat do dokumentace a v případě ověření bezproblémovosti, tyto updaty do dalších 10 dnů aplikovat na všechny systémy Objednatele,
* minimálně 2x měsíčně kontrolovat konfiguraci síťových služeb a provádět v ní změny podle aktuálního vývoje poznatků z bezpečnostního a výkonového hlediska. O každé změně provést záznam v technické dokumentaci síťových služeb,
* zajišťovat 2x měsíčně kontrolu záznamů o chybách síťových služeb a následně do 5 pracovních dnů realizovat opatření k odstranění nalezených chyb,
* zajistit spolehlivou zálohu dat dle SLA podmínek
* zajišťovat řešení provozních problémů síťových služeb
* realizovat požadavky Objednatele
* vedení technické dokumentace k systému
* vedení dokumentace incidentů

Detailní popis a specifikace požadovaných služeb:

* + - 1. **Firewall**
* zajistit dodržování bezpečnostních pravidel firewallu postavených na principu „vše zakázáno“,
* zajistit povolování komunikačních výjimek na firewallů pouze po absolvování úspěšného schvalovacího procesu. Změnu komunikačních výjimek může vždy schválit pouze odpovědná osoba ze strany Objednatele
* 1x za rok zajistit penetračních testy. Na základě výsledků penetračních testů zajistit taková opatření, která odstraní případné nedostatky nebo bezpečnostní hrozby
  + - 1. **DHCP a DNS a VPN**
* zajistit přidělování IP adresy osobám třetích stran pouze po absolvování úspěšného schvalovacího procesu. Přidělení IP adresy může vždy schválit pouze odpovědná osoba ze strany Objednatele
* minimálně 2x měsíčně provádět kontroly bezpečnostních logů VPN připojení. V případě zjištění neoprávněné aktivity, která ohrožuje bezpečnost sítě Objednatele přijmout opatření, která případnou hrozbu eliminují
  + - 1. **Routery**
* zajistit změnu komunikačních pravidel routování pouze po absolvování úspěšného schvalovacího procesu. Změnu komunikačních pravidel může vždy schválit pouze odpovědná osoba ze strany Objednatele
  + - 1. **Webové servery**
* minimálně 2x měsíčně údržba databází webových serverů
* zajistit rekonfiguraci webových serverů za účelem zprovoznění webových aplikací pouze po absolvování úspěšného schvalovacího procesu. Schválit rekonfiguraci webových serverů může vždy pouze odpovědná osoba ze strany IT Objednatele
* 1x za 6 měsíců zajistit údržbu Active Directory databází podle doporučení společnosti Microsoft
* 1x za 6 měsíců kontrolovat a zajišťovat správnou funkčnost všech doménových řadičů
  + - 1. **Aktivní infrastruktura**

Poskytování 1st level supportu pro aktivní síťovou infrastrukturu.

* na nově pořízené aktivní prvky zajišťovat do 20 pracovních dní instalace otestovaných verzí firmware, zapojení a zprovoznění do počítačové sítě Objednatele
* po vydání nových informací týkajících patchů, bezpečnostních updatů a nových funkcionalit, provést otestování těchto změn, výsledek do 2 pracovních dnů zaznamenat do dokumentace incidentů
* realizovat požadavky Objednatele
* vedení technické dokumentace k systému
* vedení dokumentace incidentů
* Zajišťovat návrhy rozvoje aktivní infrastruktury v kontextu vývoje potřeb Poskytovatele
  + - 1. **Management aktivních prvků**

V rámci managementu bude Poskytovatel zajišťovat činnost:

* 1x ročně kontrolovat konfiguraci prvků a systémů a provádět v ní změny podle aktuálního vývoje poznatků z bezpečnostního a výkonového hlediska. O každé změně provést záznam v technické dokumentaci systémů, konfigurační změny budou prováděny v nočních hodinách v termínu odsouhlaseném Objednatelem
* Pravidelně zajišťovat kontrolu záznamů o chybách provozovaných prvků a systémů a následně do 10 dní realizovat opatření k eliminaci výskytu chyb
* dle SLA podmínek zajišťovat řešení provozních problémů aktivní infrastruktury
* zálohy konfiguračních souborů před a po každé změně konfigurace
* 1x za 12 měsíců realizace profylaktické péče aktivní infrastruktury
  + - 1. **WiFi technologie a jejich provoz**

Poskytovatel zajistí provozování WiFi technologie. Provoz takovýchto zařízení musí být zajištěn pomocí dostupných technologií tak, aby neskýtal vysoká bezpečnostní rizika.

V rámci správy WiFi technologií bude Poskytovatel provádět:

* po vydání nových informací týkajících patchů, bezpečnostních updatů a nových funkcionalit, do 10 pracovních dnů provést otestování těchto změn, výsledek do 2 pracovních dnů zaznamenat do dokumentace incidentů a v případě ověření bezproblémovosti, tyto updaty do dalších 10 pracovních dnů aplikovat na všechny systémy Objednatele, Veškeré změny a následné ověření funkčnosti musí probíhat v nočních hodinách v termínu odsouhlaseném Objednatelem
* minimálně 2x měsíčně kontrolovat konfiguraci WiFi prvků a provádět v ní změny podle aktuálního vývoje poznatků z bezpečnostního a výkonového hlediska. O každé změně provést záznam v technické dokumentaci systémů, konfigurační změny budou prováděny v nočních hodinách v termínu odsouhlaseném Objednatelem
* zajišťovat 1x ročně kontrolu záznamů o chybách provozovaných prvků a systémů a následně do 10 pracovních dní realizovat opatření k eliminaci výskytu chyb
* dle SLA podmínek zajišťovat řešení provozních problémů aktivní infrastruktury
* zálohy konfiguračních souborů před a po každé změně konfigurace
  1. **Bezpečnost**

V rámci zajišťování bezpečnosti IT prostředí objednatele bude poskytovatel vykonávat:

* + 1. **Správa antispamové kontroly**

Detailní popis a specifikace požadovaných služeb:

* provádět takové konfigurační změny antispamové kontroly, které eliminují výskyt spamu v elektronické poště a zajistí bezproblémové doručování oficiálních e-mailů
* po vydání nových informací týkajících se SW patchů, bezpečnostních updatů a nových funkcionalit, do 10 pracovních dnů provést otestování těchto změn, výsledek do 2 pracovních dnů zaznamenat do dokumentace a v případě ověření bezproblémovosti, tyto updaty do dalších 5 pracovních dnů aplikovat na všechny systémy Objednatele
* minimálně 2x měsíčně kontrolovat záznamy o chybách antispamové kontroly a následně realizovat opatření k eliminaci výskytu chyb
* garantovat antispamovou kontrolu pro veškerou příchozí elektronickou poštu
* dle SLA podmínek zajišťovat řešení provozních problémů antispamové kontroly
* realizovat požadavky Objednatele
* vedení technické dokumentace k systému
* vedení dokumentace incidentů
  + 1. **Správa zálohování a archivace dat**

Detailní popis a specifikace požadovaných služeb:

* garantovat spolehlivou zálohu a archivaci dat Objednatele podle aktuálně platného zálohovacího plánu
* po vydání nových informací týkajících se SW patchů, bezpečnostních updatů a nových funkcionalit, do 10 pracovních dnů provést otestování těchto změn, výsledek do 2 pracovních dnů zaznamenat do dokumentace a v případě ověření bezproblémovosti, tyto updaty do dalších 5 pracovních dnů aplikovat na všechny systémy Objednatele
* v souladu se zálohovacím a archivačním plánem kontrolovat záznamy o chybách zálohovacích a archivačních systémů a následně realizovat opatření k eliminaci výskytu chyb
* vytvářet a následně spravovat a aktualizovat zálohovací a archivační plány, jejichž obsah je definován projektem rozvoje
* Obsah plánu:
  + specifikace zálohovaných nebo archivovaných dat, včetně objemu dat,
  + režim zálohování a archivace (full, incremental,…)
  + specifikace místa uložení zálohovaných dat a času, kdy se data zálohují a specifikace časové periodiky zálohování a archivace dat, jakým způsobem je nakládáno se zálohovacími nebo archivačními médii
  + popis jakým způsobem data obnovovat
  + popis jakým způsobem nakládat s vyřazenými zálohami (data) a zálohovacími nebo archivačními médii určenými k likvidaci
* spravovat zálohovací a archivační média takovým způsobem, aby nemohlo dojít ke ztrátě, záměně, neoprávněné manipulaci nebo fyzickému poškození
* dle SLA podmínek zajišťovat řešení provozních problémů systému zálohování a archivace dat
* realizovat požadavky Objednatele
* vedení technické dokumentace k systému
* vedení dokumentace incidentů
  + 1. **Update informačních systémů**
* po vydání nových informací týkajících se SW patchů, bezpečnostních updatů a nových funkcionalit, provést otestování těchto změn, výsledek zaznamenat do dokumentace a v případě ověření bezproblémovosti, tyto updaty aplikovat na všechny systémy Objednatele
* lhůty pro testování, zaznamenání do dokumentace a aplikaci na všechny systémy Objednatele, jsou uvedeny v odpovídajících kapitolách této smlouvy

1. **Správa Krizových plánů**

Krizové plány jsou dokumenty preventivně připravené a obsahují pracovní scénáře pro nejčastěji uvažované situace výpadků jednotlivých systémů. Výsledným dokumentem je detailní scénář, podle kterého bude obsluha (i s minimálními znalostmi) postupovat v okamžiku, kdy krizová situace nastane.

Krok za krokem tak krizový plán provede operátora procesem tak, aby jeho postup neobsahoval procesní chyby, a naopak obsahoval činnosti, které zajistí všechny úkony, potřebné k minimalizaci způsobených škod a zkrácení doby, kdy bude krizová situace vyřešena.

Forma krizových plánu musí mít přehlednou podobu a jasnou formulaci, protože jejich reálné použití se předpokládá v situacích s větší pravděpodobností pochybení.

Detailní popis a specifikace požadovaných služeb:

* zajišťovat 1x ročně aktualizaci veškerých krizových plánů pro implementované technologie Aktualizací se rozumí zdokumentování stavu a popis změn, které odpovídají postupům pro možnost snadného uplatnění procesů definovaných v krizových plánech. Zajišťovat 1x ročně prověření realizovatelnosti krizových plánů. Prověření realizovatelnosti bude probíhat fyzickou realizací popsaných procesů v krizových plánech na testovacích zařízeních. O výsledcích bude sepsána správa, která bude obsahovat informace o úspěšnosti obnovy jednotlivých oblastí IT podle krizových plánů. Bude-li shledána nefunkčnost krizových plánů, bude sjednána náprava formou předělání krizových plánů a opětovného prověření realizovatelnosti
* Seznam krizových plánů je popsán v projektu zavedení Krizových plánů, jehož realizaci Poskytovatel zajistí