**Technické specifikace**

V rámci podpory provozu ICT ČOI se požaduje poskytování služeb v oblasti správy provozovaného HW, správy provozovaného SW, dohledu WAN ČOI, konzultací a školení. Seznam níže vymezeného HW a SW může být měněn podle aktuální situace ve smyslu vyřazení „starého“ či zařazení „nového“.

**1. Rozsah provozovaného HW ČOI:**

1. Dell VRTX Chassis, fyzický počet: 4
2. DELL servery (standalone), fyzický počet: 2
3. Quantum Scala i3-i6 tape library LTO-7,
4. Fortigate firewall, Fortianalyzer,
5. Bezpečnostní sonda SSA 180,
6. Aktivní, síťové prvky Extreme Summit 4xx,
7. Aruba Wi-Fi,
8. UPS APC od 1,5 kVA do 7,5 kVA,
9. Autentizační (bezpečnostní) tokeny, poskytovatel Česká pošta, a.s.
10. HW na 7 regionálních pobočkách (České Budějovice, Ústí nad Labem, Liberec, Hradec Králové, Brno, Olomouc, Ostrava) v rozsahu:
11. standalone server DELL,
12. Fortigate Firewall
13. Aktivní, síťové prvky Extreme Summit 4xx.
14. Klientský HW (cca 500 zařízení):
15. Pracovní stanice Dell,
16. Notebooky Dell.,

**2. Rozsah provozovaného SW**

1. MS Windows server 2012 R2, 2016, 2019, služby zejména v oblasti:
i) Group Policy Object,
ii) virtualizace využitím Hyper-V( v současnosti 3 nody, cca 60 virt. serverů),

iii) Active Directory,
iv) DNS, DHCP, NPS, WSUS služby.

1. MS Exchange 2013,
2. MS SharePoint 2016,
3. MS SQL databáze 2014, 2017 (Standard, Express),
4. MS Windows 10, Office 2016,
5. DB Firebird 3.0,
6. Linux Debian 9,
7. NetSight 6.2.0.224,
8. SCDPM, SCOM, SCCM, SCVMM,
9. XMC Extreme Networks.

 **3. Rozsah „nesystémového“ provozovaného SW**

1. Agendový, kontrolní IS Mercurius, dodavatel firma INISOFT, s.r.o.,
2. Personální IS Okbase, dodavatel firma OKsystem, a.s.,
3. Spisová služba GINIS®, dodavatel firma Gordic, s.r.o.,
4. Ekonomický IS JASU® CS, dodavatel firma MÚZO Praha, s.r.o.,
5. Právní IS ASPI, dodavatel Wolters Kluwer ČR, a.s.,

**4. Rozsah bezpečnostního provozovaného SW**

1. IS pro správu SW, HW - AuditPro,
2. Antivirový IS Symantec:
i) Endpoint Protection,
ii) Endpoint Protection Manager,
iii) Messaging Gateway.
3. IS pro správu nestrukturovaných informací Varonis,
4. IS pro detekci nepovoleného SW Carbon Black,
5. Přístupový IS WIN PAK,
6. Správa identit MidPoint,
7. SW produkty pro správu Firewallu (FortiManager),
8. IS pro monitoring provozu System Center Operations Manager,
9. LOGmanager 3.x

**5. Dohled WAN ČOI**

V prostředí WAN ČOI je implementována segmentace sítě. Je nasazen protokol 802.1X. V tomto prostředí s využitím vlastností nástrojů bezpečnostního HW, SW, zejména LOGmanageru, FortiAnalyzeru, Varonisu, bezpečnostní sondy SAA 180, aktivních prvků, dohledovat vnitřní síť v s cílem:

1. návrhů opatření k předcházení incidentů narušujících bezpečnost,
2. řešení bezpečnostních incidentů a událostí,
3. poskytování součinnosti regulační autoritě k posouzení bezpečnosti,
4. exportu dat, provozních údajů (auditní stopa) spojených s provozem IS Mercurius, Okbase, EIS, GINIS dle vyžádání objednatele.

**6. Konzultace a školení**

Konzultace budou poskytovány dodavatelem v rozsahu technologií zahrnující služby dle
 kap. 1, kap. 2, kap. 4. Budou objednány emailem na adresu dodavatele.

**7. Forma poskytované služby** Všechny požadované služby budou poskytovány jednak formou měsíčního paušálu a dále
 formou objednání konkrétní služby („Ad-hoc“ služby).

**Paušální služby:**

1. instalace, konfigurace, kontrola provozu HW v rozsahu kap. č.1,
2. instalace, konfigurace, kontrola provozu SW v rozsahu kap. č.2,
3. kontrola, nastavení centrálních politik (GPO),
4. dohled WAN ČOI v rozsahu kap. č. 5a a 5b,
5. kontrola systému zálohování,
6. kontrola licenční politiky (evidence, počty, platnost licencí),
7. kontrola záruk (termíny) nového HW,
8. řádná evidence a vedení provozních deníků k jednotlivým prvkům WAN ČOI.

**Ad-hoc služby**

1. změna dislokace ÚI (jedná se pouze o podpůrné služby navazující na stěhování sídla Objednatele do pronajatých prostor), participace na zabezpečení provozu DC,
2. FAZ – reporty: modifikace stávajících, vytváření nových,
3. LOG – use case: modifikace stávajících, vytváření nových,
4. BI – reporty: modifikace stávajících, vytváření nových,
5. EA – modely ČOI: úprava stávajících, vytváření nových,
6. řešení obnovy po havárii,
7. migrace dat dle požadavků,
8. služby dle bodu 5c a 5d,
9. odborná školení, konzultace dle bodu 6.

Pozn: BI – bussines inteligence, DC – datové centrum, EA – Enterprise Architektura (jazyk

 ArchiMate), FAZ – Fortianalyzer, LOG – logmanager, ÚI – ústřední inspektorát.

**8. Klasifikace havarijních stavů**

 Havarijními stavy rozumíme jakoukoliv nefunkčnost, bezpečnostní incident či událost. Rozlišujeme 4 kategorie havarijních stavů:

|  |
| --- |
| Havarijní stav: kategorie A |
| Kybernetický incident/událost dle zákona 181/2014 Sb. Prvek IT/služba není použitelná ve svých základních funkcích nebo se vyskytuje funkční závada znemožňující používání služby. Tento stav může ohrozit běžný provoz, případně může způsobit větší finanční nebo jiné škody. |
| Havarijní stav: kategorie B |
| Prvek IT/služba je ve svých funkcích degradována tak, že tento stav omezuje běžný provoz. |
| Havarijní stav: kategorie C  |
| Ostatní incidenty/vady které nespadají do kategorií A a/nebo B a které nejsou způsobeny software třetích stran.  |
| Havarijní stav: kategorie D  |
| Incidenty/vady, které jsou způsobeny software třetích stran. |

Pozn: Havarijní stavy způsobené „3. mocí“ tzn. totální zničení DC (požár, zemětřesení, výbuch,
 voda) nejsou řešeny touto smlouvou.

**9. Parametry SLA**

|  |  |  |  |
| --- | --- | --- | --- |
| **Kategorie h. stavů** | **Potvrzení převzetí požadavku** | **Garantovaná doba zahájení prací**  | **Garantovaná doba vyřešení po řádném nahlášení** |
| A | do 1 hod. | 2 hod. | Nejpozději do 24 hod. |
| B | do 1 hod. | 4 hod. | Následující pracovní den |
| C | do 1 hod. | Následující pracovní den | Do 5 pracovních dnů |
| D |  do 1 hod. | Následující pracovní den | BE (Best Effort) dle možností v co nejkratší době |

Do doby vyřešení incidentu se nezapočítává:

1. čekání poskytovatele na vyžádanou součinnost objednatele,
2. prodlevy způsobené závadami na zařízeních mimo rozsah systémů, na nichž poskytovatel drží podporu,
3. prodleva způsobená zásahem vyšší moci.

**10. Sankce za nedodržení podmínek SLA**

 U havarijních stavů je Objednatel oprávněn uplatnit vůči Dodavateli sankci za nedodržení
 parametrů SLA dle následující tabulky:

|  |  |
| --- | --- |
| Kategorie incidentu | Výše sankce |
| A | 15 000,- Kč |
| B | 10 000,- Kč |
| C |  5 000,- Kč |
| D |  1 000,- Kč |

**11. Způsob zadávání požadavků** (havarijní stavy, požadavek na Ad-hoc služby)

Objednatel může kontaktovat dodavatele minimálně tímto způsobem:

* prostřednictvím formuláře v aplikaci Helpdesk dodavatele dostupný 24x7x365,
* telefonem na hotline dodavatele dostupný 24x7x365,
* e-mailem na dodavatele dostupný 24x7x365,
* osobně při návštěvě v místě dodavatele.

**12. Poskytování služeb helpdesku a hotline dodavatelem**

 **a) helpdesk**

* webová aplikace provozovaná dodavatelem s vysokou dostupností,
* každý tiket a jakákoliv změna musí být evidována včetně času a původce,
* schvalovací řízení je součástí aplikace,
* tikety jsou automaticky distribuovány na jednotlivé řešitele dodavatele,
* počet uživatelů, řešitelů a schvalovatelů není omezen,
* aplikace má schopnost reportingu tiketů dále elektronicky zpracovatelných (MS Excel).

 **b) hotline**

* hotline musí být provozována z české republiky s česky mluvícími operátory,
* hotline poskytuje na vyžádání informaci o průběhu řešení tiketu.