Evidenční č. smlouvy Objednatele: S-263-030/2019
Č. j.: 1/2019-030-SML/1
Výtisk č.: 1

Smlouva o poskytování služeb

„Aktualizace systému DOK a poskytnutí technické podpory"

uzavřená podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník (dále jen „Občanský zákoník")

Článek I.

Smluvní strany

1. **Česká republika - Ministerstvo dopravy**

Sídlo:	nábřeží Ludvíka Svobody 1222/12, 110 15 Praha 1
IČO:	66003008
DIČ:	CZ66003008
Zastoupena:	[redacted]
Bankovní spojení:	ČNB Praha 1, Na Příkopě 28
č. účtu:	[redacted]

(dále jen „Objednatel")

2. **WAK System, spol. s r.o.**

Sídlo:	[redacted]
IČO:	25720384
DIČ:	CZ25720384
Zastoupena:	[redacted]
Bankovní spojení:	Raiffeisenbank, a.s.
č. účtu:	[redacted]
Datum registrace:	16.12.1998
Spisová značka:	oddíl C, vložka 64160 vedená u Městského soudu v Praze

(dále jen „Poskytovatel")

Článek II.

Předmět smlouvy

1. Předmětem této smlouvy je závazek Poskytovatele zajistit pro Objednatele služby aktualizace a technické podpory informačního systému Dopravní informační systém DOK (dále jen „DOK") podle specifikace uvedené v odst. 2. tohoto článku smlouvy, a závazek Objednatele za řádně poskytnuté služby zaplatit Poskytovateli dohodnutou cenu podle čl. V. této smlouvy.
2. Předmětem této smlouvy je zajištění následujících služeb rozdělených do dvou oblastí:

Oblast I – Aktualizace systému DOK

Předmětem Aktualizace systému DOK je zajištění podmínek kybernetické bezpečnosti a implementace nařízení GDPR.

I.1 Veřejná část systému DOK

Předmětem aktualizace veřejné části systému DOK bude:

- Konverze databází systému DOK za účelem provozu systému v prostředí vyšší verze SQL Serveru. Verze SQL serveru bude určena Objednatelem v objednávce dodávky a bude vyhovovat požadavkům kybernetické bezpečnosti.
- Odstranění asp stránek s nutností autentizace zobrazování dat v mapových podkladech a s tím souvisejících funkčností.
- Konverze komponent systému DOK pro prostředí platformy .NET 4 (akt. runtime a zajištění verze release).
- Kontrola funkčnosti systému po provedených konverzích včetně funkčnosti systému na protokolu https.
- Implementace opatření proti útokům SQL injection a Cross Site Scripting parametrizací dotazů a auditem skriptů jednotlivých asp stránek (cca 100 asp souborů).
- Kontrola funkčnosti a bezpečnosti systému po provedených úpravách.
- Instalace a ověření funkčností systému DOK a jeho bezpečnosti v novém systémovém prostředí Objednatele. Realizace opatření proti případným zjištěným zranitelnostem.

I.2 Implementace Nařízení GDPR u celého systému DOK

Předmětem implementace bude:

- Fyzické odstranění všech osobních údajů z celého systému DOK.
- Úprava formulářů s ohledem na odstranění osobních údajů.
- Odstranění odkazu na databázi bezpečnostních poradců.
- Vizuální kontrola obsahu Název a Poznámka části Ekologické havárie (38.000 záznamů) a vymazání osobních údajů (jména osob, registrační značky dopravních prostředků, rodná čísla, atd.).
- Kontrola funkčnosti a bezpečnosti systému po provedených úpravách.
- Instalace a ověření funkčností systému DOK a jeho bezpečnosti v novém systémovém prostředí Objednatele. Realizace opatření proti případným zjištěným zranitelnostem.

Oblast II – Zajišťování pravidelné technické podpory systému DOK

Předmětem pravidelné technické podpory systému DOK bude:

- Hotline – libovolného rozsahu.
- Vzdálená čtvrtletní servisní údržba databáze a softwarová prohlídka systému.
- Práce (dle oboustranně potvrzeného předávacího protokolu) související se zabezpečením rutinního provozu systému v celkovém rozsahu 10 hodin/rok:
  - Nasazení aktualizací softwarových komponent, které nejsou standardní součástí operačního systému.
  - Spolupráce při nasazování aktualizací softwarových komponent, které jsou standardní součástí operačního systému, řešení případných nekompabilit.
  - Spolupráce při odstraňování zranitelností, které budou zjištěny v komponentách aplikace.

3. Předmět plnění musí být Poskytovatelem předán Objednateli v řádném a provozuschopném stavu, bez vad a zjevných nedodělků, a to včetně procesu akceptace Objednatelem.
4. Podkladem pro akceptaci bude „Předávací protokol Poskytovatele".

Článek III.

Doba, místo a způsob plnění

1. Služby je Poskytovatel povinen poskytovat průběžně od data účinnosti smlouvy (dle článku XIV. odst. 1 této smlouvy) v následujících termínech:
   a) Oblast I – Aktualizace systému DOK

      Etapa I. 1: do tří měsíců ode dne účinnosti této smlouvy

      Etapa I. 2: do tří měsíců ode dne účinnosti této smlouvy

      Plnění služeb bude realizováno formou vzdálené instalace úpravy do připraveného systémového prostředí určeného serveru. Předání provedených služeb bude oznámeno odpovědným osobám Objednatele (dle článku VII. této smlouvy) elektronicky, pomocí emailové zprávy formou „Předávacího protokolu Poskytovatele".

   b) Oblast II – Zajišťování pravidelné technické podpory systému DOK od následujícího měsíce, kdy bylo ze strany Objednatele akceptováno plnění dle čl. III odst. 1 písm. a) a to po dobu 48 měsíců.

      Plnění služeb bude realizováno formou servisního zásahu pomocí vzdáleného přístupu nebo v rámci osobní návštěvy pověřeného pracovníka Poskytovatele v systémovém prostředí určeného serveru. Předání provedených služeb bude oznámeno odpovědným

osobám Objednatele (dle článku VII. této smlouvy) elektronicky, pomocí emailové zprávy formou „Předávacího protokolu Poskytovatele".

2. Smlouva se uzavírá na dobu 51 měsíců od data její účinnosti dle čl. XIV. odst. 1 této smlouvy popř. do vyčerpání částky ve výši maximální celkové ceny smlouvy dle čl. V odst. 1 této smlouvy, nastane-li dříve.
3. Místem plnění předmětu smlouvy je sídlo Objednatele.
4. Požadavky na Poskytovatele mohou vznášet písemně pouze oprávněné osoby Objednatele:

[redacted]

Případné změny oprávněných osob budou Poskytovateli sděleny písemně.

5. Objednatel je povinen do jednoho měsíce od data účinnosti smlouvy (dle článku XIV. odst. 1 této smlouvy) zajistit pro Poskytovatele aktuální verze Windows a SQL serveru, včetně zajištění vzdáleného přístupu pro administrátory IS DOK (prostřednictvím serveru na vnitřní síti)
6. Zajištění systémového prostředí bude oznámeno odpovědným osobám Poskytovatele (dle článku VII. této smlouvy) elektronicky prostřednictvím e-mailové zprávy, která bude obsahovat systémové parametry prostředí a SQL Serveru, přístupové údaje a nastavená přístupová oprávnění.
7. Povinnosti vyplývající z Přílohy č. 4 této smlouvy se vztahují pouze k prostředí spravovanému Poskytovatelem. Zálohování provádí Objednatel.
8. Dokumentace bude provedena v souladu s ustanovením článku 8 Přílohy č. 3 této smlouvy a bude obsahovat zejména:
   - administrátorskou dokumentaci, včetně instalačního manuálu
   - konfiguraci použitého HW a SW pro provoz

Článek IV.

Schválení poskytnutých služeb

1. Poskytovatel splní svou povinnost řádně poskytnout služby dnem, kdy je příslušná činnost řádně vykonána a její výstup je akceptován Objednatelem dle odst. 2 tohoto článku.

2. Řádné splnění povinností Poskytovatele osvědčí Objednatel podpisem Akceptačního protokolu u oblasti I jednorázově a u oblasti II za každé 3 kalendářní měsíce, přičemž každá ze stran obdrží po jednom jeho vyhotovení. Časová náročnost plnění předmětu smlouvy dle čl. II. této smlouvy musí být v Akceptačním protokolu vyčíslena v členění na jednotlivé činnosti.

   Akceptační protokol musí obsahovat minimálně tyto informace:

   - soupis provedených služeb,
   - doba strávená řešením
   - informaci, zda výstupy byly Objednatelem akceptovány, akceptovány s výhradami, či neakceptovány,
   - datum akceptace,
   - podpisy odpovědných osob za obě strany.

3. Zjistí-li Objednatel v plnění Poskytovatele nebo při předání výstupů služeb zjevné vady, je povinen o tom sepsat zápis s uvedením zjištěných vad, podepsaný oprávněnou osobou Objednatele. V takovém případě je lhůta Poskytovatele na analýzu zjištěných vad 10 pracovních dnů od doručení tohoto zápisu.
4. Lhůta pro odstranění zjištěných vad činí 10 pracovních dnů ode dne doručení tohoto zápisu Poskytovateli. Do doby odstranění vad není Objednatel povinen podepsat Akceptační protokol ani zaplatit cenu za poskytnuté služby.
5. Pokud Objednatel do 10 pracovních dnů po předání výstupů služeb neakceptuje poskytnuté plnění nebo nepředá Poskytovateli zápis s uvedenými zjištěnými vadami, je Poskytovatel povinen Objednatele písemně vyzvat k akceptaci nebo k oznámení případných vad. Pokud Objednatel v dodatečné lhůtě 10 pracovních dnů ode dne doručení oznámení Poskytovatele podle předchozí věty nepředá Poskytovateli zápis s uvedenými zjištěnými vadami, je plnění Poskytovatele považováno za akceptované Objednatelem.

Článek V.

Celková cena

1. Smluvní strany se dohodly, že celková cena za poskytování služeb, nepřesáhne částku ve výši 248.400,- Kč bez DPH, tj. 300.564,- Kč s DPH. Detail ceny je uveden v Příloze č. 1, která je nedílnou součástí této smlouvy.

2. Ceny dle tohoto článku jsou cenami maximálními a nepřekročitelnými a zahrnují veškeré náklady Poskytovatele související s plněním předmětu této smlouvy.
3. V případě změny DPH dané právními předpisy bude k ceně bez DPH přiúčtována daň dle sazby platné ke dni zdanitelného plnění.

Článek VI.
Platební a fakturační podmínky

1. Cena za plnění předmětu této smlouvy bude Objednatelem placena na základě Poskytovatelem řádně vystavené faktury, po ukončení jednotlivých etap (včetně akceptace Objednatelem) dle čl. III. odst. 1 písm. a) této smlouvy, resp. za každé 3 kalendářní měsíce zpětně v případě plnění dle čl. III. odst. 1 písm. b) této smlouvy.
2. Dnem platby se rozumí den, kdy je fakturovaná částka odeslána z účtu Objednatele na účet Poskytovatele uvedený na faktuře, který musí odpovídat číslu uvedenému v záhlaví této smlouvy nebo číslu účtu uvedenému v registru plátců DPH. Případnou změnu čísla účtu je Poskytovatel povinen Objednateli písemně oznámit a na zpětný dotaz Objednatele opětovně písemně potvrdit, jinak je Objednatel oprávněn fakturu vrátit Poskytovateli podle odst. 7 tohoto článku.
3. Objednatel nebude poskytovat Poskytovateli žádné zálohy na cenu za plnění předmětu smlouvy v jakékoli formě.
4. Smluvní strany se dohodly na době splatnosti jednotlivých faktur 30 kalendářních dnů ode dne jejich doručení Objednateli. Faktury Poskytovatele budou předávány elektronicky na emailovou adresu Objednatele [redacted] ebo datovou schránkou.
5. Oprávnění fakturovat cenu vznikne Poskytovateli po odsouhlasení a převzetí plnění Objednatelem formou Akceptačního protokolu, jehož kopii je Poskytovatel povinen k faktuře připojit.
6. Faktura vystavená Poskytovatelem musí obsahovat náležitosti daňového dokladu stanovené právními předpisy, evidenční číslo a název smlouvy Objednatele. Poskytovatel bude fakturovat poskytnuté služby zvlášť, resp. v členění dle jednotlivých služeb uvedených v Příloze č. 1 této smlouvy.
7. V případě, že faktura nebude obsahovat stanovené náležitosti, anebo údaje v ní obsažené budou chybné, je Objednatel oprávněn zaslat ji ve lhůtě splatnosti zpět Poskytovateli k doplnění či opravě, aniž se tím dostane do prodlení s jejím zaplacením; lhůta splatnosti počíná běžet znovu ode dne doručení bezvadné faktury Objednateli.

Článek VII.

Odpovědné osoby

Osoby odpovědné za řádné splnění povinností dle této smlouvy jsou:

- na straně Poskytovatele:

- na straně Objednatele:

Článek VIII.

Povinnosti a práva Poskytovatele

1. Poskytovatel je povinen spolupracovat s oprávněnými pracovníky Objednatele ve věci plnění předmětu této smlouvy.
2. Poskytovatel je povinen na požádání informovat Objednatele o průběhu plnění předmětu této smlouvy akceptovat nebo řádně vypořádat jeho doplňující pokyny a připomínky související s plněním předmětu této smlouvy.
3. Zjistí-li Objednatel v průběhu plnění předmětu této smlouvy nedostatky, je Poskytovatel povinen na písemnou výzvu tyto nedostatky bezodkladně odstranit nebo řádně vypořádat bez nároku na navýšení celkové ceny, nejdéle však do 10 pracovních dnů ode dne doručení výzvy.
4. Poskytovatel je povinen upozornit Objednatele na nevhodnost jím udělených pokynů, jestliže tuto nevhodnost mohl zjistit při vynaložení odborné péče. Poskytovatel je však povinen pokyny Objednatele splnit, trvá-li na tom Objednatel i přes jeho upozornění, v takovém případě však Poskytovatel neodpovídá za tím vzniklou škodu.

5. Poskytovatel je oprávněn svolávat po dohodě s Objednatelem pracovní schůzky k řešení sporných otázek, souvisejících s plněním předmětu smlouvy.
6. Poskytovatel je povinen na požádání konzultovat v průběhu realizace plnění s Objednatelem přijatá řešení a to nejpozději do 5 pracovních dnů ode dne doručení písemné žádosti. Poskytovatel zajistí pro takovéto konzultace účast kvalifikovaných pracovníků.
7. Poskytovatel je oprávněn vyjadřovat se písemně k předkládaným písemným materiálům Objednatele, a to nejpozději do 5 pracovních dnů od jejich doručení, pokud není písemně dohodnuto jinak.
8. Poskytovatel je povinen bezodkladně a s vyvinutím největšího úsilí řešit ve spolupráci s Objednatelem překážky v plnění předmětu této smlouvy.
9. Poskytovatel odpovídá za to, že pracovníci plnící předmět této smlouvy mají pro stanovenou práci odbornou způsobilost a budou dodržovat platné právní předpisy. Poskytovatel je povinen dodržovat vnitřní předpisy Ministerstva dopravy, pokyny Objednatele týkající se pohybu osob po budově a provozu budovy a seznámit s nimi všechny pracovníky plnící předmět této smlouvy, kteří se budou v souvislosti s plněním předmětu této smlouvy v budově Ministerstva dopravy pohybovat. Poskytovatel odpovídá za škodu způsobenou nedodržením těchto předpisů jeho pracovníky.
10. Poskytovatel je povinen plnit předmět smlouvy řádně, včas a s odbornou péčí, na vlastní odpovědnost, podle svých nejlepších znalostí a schopností a v souladu s obecně závaznými právními předpisy, přičemž je povinen sledovat a chránit oprávněné zájmy Objednatele.
11. Poskytovatel je oprávněn užít ke splnění svých závazků z této smlouvy třetích osob pouze na základě předchozího písemného souhlasu Objednatele, vždy však odpovídá, jako by poskytoval plnění sám.
12. Poskytovatel odpovídá Objednateli za škodu, kterou mu způsobil v souvislosti s poskytováním služeb prokázaným porušením svých povinností podle této smlouvy. Pro účely této smlouvy se za škodu považují rovněž peněžité sankce uložené Objednateli jakýmkoliv národním orgánem nebo orgánem EU.
13. Veškerá práva k užití plnění předmětu smlouvy přecházejí na Objednatele jejich řádným předáním a převzetím. Poskytovatel není oprávněn výstupy plnění této smlouvy zveřejňovat ani přenechat třetí osobě bez předchozího písemného souhlasu Objednatele. Zveřejnění nebo přenechání výstupu plnění předmětu smlouvy nebo jeho části Poskytovatelem třetí osobě bez předchozího písemného souhlasu Objednatele je důvodem pro odstoupení Objednatele od této smlouvy dle čl. XI. odst. 2 této smlouvy.

14. Poskytovatel je oprávněn uvádět systém DOK, jako svoje dílo vytvořené pro Objednatele (pouze pro obchodní prezentaci nebo reference provedených prací v rámci obchodních nabídek).
15. V případě, že bude Objednatel v prodlení s plněním dle čl. III odst. 5 této smlouvy, budou o počet dnů prodlení Objednatele posunuty časové lhůty Poskytovateli pro plnění dle čl. III odst. 1 této smlouvy.

Článek IX.
Povinnosti a práva Objednatele

1. Objednatel se zavazuje poskytnout Poskytovateli potřebné podklady, odborné konzultace a součinnost nutnou k plnění předmětu této smlouvy.
2. Objednatel se zavazuje umožnit vstup pracovníkům Poskytovatele na pracoviště Objednatele během jeho pracovní doby za účelem plnění předmětu této smlouvy.
3. Objednatel je oprávněn svolávat po dohodě s Poskytovatelem pracovní schůzky k řešení sporných otázek, souvisejících s plněním předmětu smlouvy.
4. Objednatel bude na požádání konzultovat v průběhu realizace plnění s Poskytovatelem přijatá řešení a to nejpozději do 10 pracovních dnů od doručení písemné žádosti, pokud není dohodnuto jinak. Objednatel zajistí pro takovéto konzultace účast kvalifikovaných pracovníků.
5. Objednatel je oprávněn vyjadřovat se písemně k předkládaným písemným materiálům Poskytovatele, a to nejpozději do 10 pracovních dnů od jejich doručení, pokud není dohodnuto jinak. Připomínky Objednatele je Poskytovatel povinen náležitě vypořádat.
6. Objednatel poskytne na vyžádání Poskytovateli konzultaci k bezpečnostnímu testování systému DOK, a to nejpozději do jednoho měsíce ode dne vyžádání.

Článek X.
Smluvní pokuta, úrok z prodlení

1. V případě prodlení Objednatele s úhradou řádně vystavené faktury je Objednatel povinen zaplatit Poskytovateli úrok z prodlení v zákonné výši z dlužné částky za každý započatý den prodlení.
2. V případě prodlení Poskytovatele s řádným poskytnutím služeb v termínu stanoveném dle čl. III. odst. 1 této smlouvy nebo s plněním povinností stanovených v čl. VIII. odst. 3 této smlouvy, je Poskytovatel povinen zaplatit Objednateli smluvní pokutu ve výši 100,- Kč

za každý započatý den prodlení. V případě porušení povinnosti stanovených v čl. VIII. odst. 13 zaplatí Poskytovatel Objednateli smluvní pokutu ve výši 10.000,- Kč.

3. Smluvní pokuta a úrok z prodlení jsou splatné ve lhůtě 30 kalendářních dnů ode dne doručení jejich vyúčtování druhé smluvní straně.
4. Zaplacením smluvní pokuty není dotčen nárok Objednatele na náhradu škody ani povinnost Poskytovatele řádně dokončit příslušné plnění předmětu smlouvy, popř. odstranit vady.

Článek XI.

Ukončení smlouvy, odstoupení od smlouvy

1. Smluvní vztah vzniklý na základě této smlouvy lze ukončit těmito způsoby:
   a) písemným odstoupením od smlouvy za podmínek uvedených v § 2002 Občanského zákoníku v případě podstatného porušení smlouvy druhou smluvní stranou,
   b) písemným odstoupením od smlouvy v souladu s § 2001 Občanského zákoníku v případě porušení smluvních povinností druhou smluvní stranou uvedených v odst. 2 tohoto článku smlouvy.
   c) písemnou dohodou smluvních stran v souladu s § 1981 Občanského zákoníku,
   d) písemnou výpovědí.
2. Smluvní strany se dohodly, že jsou oprávněny odstoupit od smlouvy dle odst. 1 písm. b) tohoto článku:
   a) Objednatel v případě porušení povinností Poskytovatele stanovených v čl. VIII. odst. 8, 9, 10 nebo 13 této smlouvy,
   b) každá ze smluvních stran v případě porušení povinností druhou smluvní stranou stanovených v čl. XII odst. 1 nebo čl. XIV odst. 4 této smlouvy.
3. Účinky odstoupení od smlouvy nastávají dnem doručení písemného oznámení o odstoupení druhé smluvní straně.
4. Kterákoliv smluvní strana může tuto smlouvu písemně vypovědět bez uvedení důvodu s jednoměsíční výpovědní lhůtou, která počíná běžet dnem doručení písemné výpovědi druhé smluvní straně. Vypovědět smluvní vztah lze nejdříve po dokončení oblasti I.
5. Ukončením smlouvy není dotčen nárok na zaplacení smluvní pokuty nebo úroku z prodlení, pokud již dospěl, případně nárok na náhradu škody vzniklé porušením této smlouvy.

Článek XII.

Další ujednání

1. Žádná ze smluvních stran není oprávněna poskytnout třetím osobám jakékoliv informace o podmínkách této smlouvy a souvisejících s touto smlouvou, jejichž obsahem mohou být důvěrné informace, osobní a citlivé údaje, informace týkající se obchodního tajemství, technologie nebo know-how, s výjimkou povinnosti poskytovat informace podle zvláštních předpisů. Ustanovení odst. 5 tohoto článku tím není dotčeno.
2. Závazky dle předchozího odstavce tohoto článku zůstávají v platnosti i po ukončení účinnosti této smlouvy.
3. Dnem předání jakéhokoliv plnění Poskytovatelem Objednateli dle smlouvy, které naplňuje znaky autorského díla podle příslušných právních předpisů, uděluje Poskytovatel Objednateli, jakož i dalším osobám, které mají tohoto plnění pro účely Smlouvy využívat, oprávnění k užití (licenci) takovéhoto plnění všemi způsoby nezbytnými pro účely smlouvy bez množstevního nebo územního omezení. Tato licence je ke každé části plnění akceptované podle smlouvy udělena jednorázově jako licence nevýhradní, neodvolatelná a udělená na celou dobu trvání majetkových práv k dílu. Odměna Poskytovatele za poskytnutí licence je zahrnuta v ceně za poskytování služeb. Součástí licence je i souhlas Poskytovatele udělený Objednateli k provedení jakýchkoliv změn nebo modifikací uvedeného plnění, a to i prostřednictvím třetích osob, a souhlas k poskytnutí oprávnění užít toto plnění třetím osobám dle uvážení Objednatele, oprávnění spojit plnění s jiným autorským dílem, zařadit do jiného díla, zařadit do souborného díla a takto je užít způsobem dle tohoto odstavce, oprávnění k rozmnožování plnění, oprávnění k užívání zdrojových kódů a dokumentace plnění včetně jejich poskytnutí třetím osobám pro dobu po ukončení této smlouvy.
4. Poskytovatel je povinen Objednateli předat veškeré aktuální zdrojové kódy provozované aplikace a technickou dokumentaci, na jejichž základě bude mít Objednatel možnost provést případný další rozvoj bez součinnosti s Poskytovatelem. Veškerá data jsou ve vlastnictví Objednatele.
5. Poskytovatel bere na vědomí a souhlasí s tím, že Objednatel v souladu se zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů, uveřejní celé znění smlouvy, včetně jejich příloh, změn a dodatků v registru smluv.

Článek XIII.

Ochrana osobních údajů

1. Smluvní strany se po dobu zpracování osobních údajů zavazují dodržovat povinnosti stanovené v Nařízení EU č. 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „Nařízení GDPR").
2. Budou-li informace poskytnuté Objednatelem či třetími stranami, které jsou nezbytné pro plnění dle této smlouvy, obsahovat údaje podléhající režimu zvláštní ochrany podle Nařízení GDPR, je Poskytovatel povinen zajistit ochranu poskytnutých údajů podle Nařízení GDPR, zejména:

   a) je oprávněn v rámci plnění předmětu této smlouvy zpracovávat osobní údaje pouze v rozsahu nezbytném pro řádné plnění předmětu této smlouvy;

   b) není oprávněn zpracování osobních údajů v rámci plnění předmětu této smlouvy svěřit, a to ani zčásti, jiné osobě bez předchozího písemného souhlasu Objednatele. V případě svěření zpracování osobních údajů jiné osobě odpovídá Poskytovatel za to, že tato osoba zajistí ochranu osobních údajů ve stejném rozsahu jako je Poskytovatel povinen podle této smlouvy;

   c) postupovat v souladu s pokyny Objednatele stanovenými pro zpracování osobních údajů;

   d) zavázat mlčenlivostí veškeré osoby podílející se na zpracování osobních údajů;

   e) přijmout veškerá opatření k ochraně zabezpečení zpracování osobních údajů uvedená zejména v čl. 32 Nařízení GDPR;

   f) poskytovat objednateli součinnost nezbytnou pro splnění povinností Objednatele vůči subjektům osobních údajů při výkonu jejich práv podle kapitoly III. Nařízení GDPR a pro zabezpečení ochrany osobních údajů podle čl. 32 až 36 Nařízení GDPR;

   g) poskytnout Objednateli veškeré informace nezbytné k doložení splnění povinností podle tohoto článku;

   h) vést záznamy o zpracování osobních údajů, které Poskytovatel provádí pro Objednatele;

i) neprodleně Objednateli oznámit případnou ztrátu, poškození, nebo neoprávněné zpřístupnění osobních údajů, popř. jakýkoliv jiný bezpečnostní incident dle Nařízení GDPR ve svěřené oblasti zpracování osobních údajů;

j) umožnit provedení auditů a kontrol plnění povinností podle tohoto článku Objednatelem nebo jím pověřenou osobou a poskytnout k tomu nezbytnou součinnost;

k) dodržovat další povinnosti a podmínky stanovené Nařízením GDPR v souvislosti se zpracováním a ochranou osobních údajů;

l) pokud podle názoru Poskytovatele určitý pokyn Objednatele porušuje Nařízení GDPR nebo jiné obecně závazné předpisy týkající se ochrany osobních údajů, je Poskytovatel povinen o této skutečnosti Objednatele neprodleně informovat;

m) při ukončení zpracovávání osobních údajů v souladu s touto Smlouvou je Poskytovatel povinen zlikvidovat veškeré poskytnuté osobní údaje a osobní údaje zpracovávané v rámci plnění předmětu této smlouvy.

Článek XIV.
Závěrečná ustanovení

1. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem uveřejnění v registru smluv.
2. Závazkové vztahy vzniklé podle této smlouvy a na jejím základě se řídí zejména Občanským zákoníkem.
3. Tuto smlouvu lze měnit, upravovat či doplňovat pouze formou písemných, vzestupně číslovaných dodatků, odsouhlasených a podepsaných oběma smluvními stranami. Tyto dodatky se stávají nedílnou součástí této smlouvy.
4. Žádná ze smluvních stran není oprávněna postoupit či jinak převést svá práva nebo povinnosti vyplývající z této smlouvy bez předchozího písemného souhlasu druhé smluvní strany.
5. Tato smlouva je vyhotovena ve čtyřech (4) vyhotoveních s platností originálu, z nichž Objednatel obdrží tři (3) a Poskytovatel jedno (1) vyhotovení.
6. Nedílnou součástí této smlouvy je následující příloha:
   Příloha č. 1: Cenová tabulka
   Příloha č. 2: Kontrolní list smlouvy dle vyhl. č. 82/2018 Sb., o kybernetické bezpečnosti (VoKB)

Příloha č. 3: Architektonické principy Ministerstva dopravy

Příloha č. 4: Pravidla pro provozovatele IS (BPI-04)

V Praze, dne.....08.-10- 2019

[redacted]

V Praze, dne.....08.-10- 2019

[redacted]

Příloha č. 1 Smlouvy

Cenová tabulka

Položka	Cena v Kč bez DPH za jednotku	Jednotka	Počet jednotek	Cena v Kč bez DPH za celkový počet jednotek	Výše DPH 21% v Kč	Cena v Kč včetně DPH za celkový počet jednotek
I. Aktualizace systému DOK	1.350,-	1 hodina	120	162.000,-	34.020,-	196.020,-
II. Technická podpora provozu systému DOK	1.800,-	1 měsíc	48	86.400,-	18.144	104.544,-
CELKEM				248.400,-	52.164,-	300.564,-

Příloha č 2 k č.j.: 1/2019-030-SML/1

Kontrolní list smlouvy dle vyhl. č. 82/2018 Sb., o kybernetické bezpečnosti (VoKB)

Smlouva o poskytování služeb „Aktualizace systému DOK a poskytnutí technické podpory", ev. č. S-263-030/2019

Smlouva dle VoKB obsahuje tato ustanovení:

- bezpečnost informací – **čl. XII, odst. 1 – osobní a citlivé údaje, čl. XIII. - GDPR, přílohou smlouvy jsou Pravidla pro provozovatele IS (BPI-04), Architektonické principy Ministerstva dopravy,**
- oprávnění užívat data – **čl. XII, odst. 4- Další ujednání**
- o autorství kódu a licencích – **čl. XII, odst. 3 a 4, čl. XII, odst. 4**
- o kontrole a auditu dodavatele – **čl. VIII – realizační tým, čl. XIII, odst. 2, písm. j)**
- o pravidlech případného řetězení dodavatelů (zachování povinností) – **čl. VIII, odst. 11**
- o povinnosti dodržovat BPI MD a Architektonické principy MD – tyto dokumenty jsou **přílohou smlouvy v aktuálním znění**
- o řízení změn – **čl. IV – schválení poskytnutých služeb, čl. VIII – povinnosti a práva poskytovatele, čl. IX – povinnosti a práva objednatele**
- o souladu smlouvy s právními předpisy – **čl. V, odst. 3, čl. VIII, odst. 9 a 10, čl. XII. odst. 5 - sledování a realizace legislativních změn, Přílohy č. 3 a č. 4**
- o povinnosti dodavatele/provozovatele řídit incidenty, řídit rizika a informovat – **čl. VIII – povinnosti a práva poskytovatele, čl. IX – povinnosti a práva objednatele**
- o významných změnách na straně dodavatele/provozovatele – **čl. III – doba, místo a způsob plnění, čl. VII – odpovědné osoby**
- o ošetření případného ukončení smlouvy z pohledu bezpečnosti informací (exit plán) – **čl. XII - další ujednání**
- o řízení kontinuity (havarijní plány) – **obsaženo v Pravidlech pro provozovatele IS a Architektonických principech Ministerstva dopravy**
- o specifikaci formátů dat a provozních informací pro předávání správci (kontinuální i na vyžádání) – **čl. III, odst. 1, 5 a 6, čl. IV, odst. 2, čl. IX, odst. 6, technická data podle Pravidel pro provozovatele IS**
- o pravidlech pro likvidaci dat – **čl. XII, odst. 1, 2 – další ujednání, čl. XIII, odst. 2, písm. m), čl. XIV, odst. 4**
- o právu jednostranně odstoupit od smlouvy (zejména v případě významné změny kontroly nad dodavatelem, resp. nad jeho základními aktivy) - **čl. XI, odst. 1, 2, 3 a 4**
- o sankcích za porušení povinností – **čl. VIII, odst. 12, čl. X – smluvní pokuta, úrok z prodlení, čl. XI, odst. 5**

Datum: [redacted]

Podpis: [redacted]

ČESKÁ REPUBLIKA MINISTERSTVO DOPRAVY	**Nařízení náměstka Sekce legislativně právní č. SŘKB/1**	**Datum účinnosti: 22. 1. 2019**

Architektonické principy Ministerstva dopravy

Vydáno náměstkem Sekce legislativně právní

dne 22. 1. 2019

č. j. 1/2019-330-RDK/1

ČESKÁ REPUBLIKA MINISTERSTVO DOPRAVY	**Nařízení náměstka Sekce legislativně právní č. SŘKB/1**	**Datum účinnosti:** **22. 1. 2019**

OBSAH

ČLÁNEK 1 POUŽITÉ ZKRATKY A SEZNAM PŘÍLOH

1.1 Použité zkratky/pojmy

Zkratka	Význam
MD	Ministerstvo dopravy České republiky
BPI MD	Bezpečnostní politika informací Ministerstva dopravy
MV	Ministerstvo vnitra České republiky
KB	Kybernetická bezpečnost
OHA MV	Odbor hlavního architekta MV
IS	Informační systém
RFC	Request For Comments, tj. žádost o komentáře
VLAN	Virtuální lokální počítačová síť
HelpDesk	Kontaktní místo pro uživatele IS MD, určené pro předávání informací o incidentech, požadavcích na úpravy IS a podobně
NDA	Dohoda o mlčenlivosti
vendor lock	Situace, kdy je zákazník závislý na určitém dodavateli nebo dodavatelích a nemůže přejít k jiným dodavatelům nebo využívat jiný produkt bez značných nákladů na tuto změnu ať již z právních či technických důvodů
IPS	Systém pro detekci a prevenci průniku
SIEM	Řízení bezpečnostních informací a událostí
Právní předpisy	Jedná se zejména o zákon č. 365/2000 Sb. ve znění prováděcích předpisů, zákon č. 181/2014 Sb. ve znění prováděcích předpisů, zákon č. 250/2017 Sb. ve znění prováděcích předpisů, nařízení GDPR aj.
WSDL	Popis rozhraní webové služby
HTTP	Hypertextový přenosový protokol
trace	Metoda protokolu HTTP
TCP	Transportní vrstva internetového protokolu
UDP	Uživatelský datagramový protokol
firewall	Část počítačové sítě, která zvyšuje bezpečnost síťového provozu
IP	Internetový protokol
IPv4, IPv6	Vylepšené verze internetového protokolu IP
URL	Adresa určující umístění prostředku/dokumentu na internetu
proxy server	Počítačové zařízení, které slouží k propojení webového prohlížeče a internetu
Hyper-V	Označení pro jednu z technik virtualizace hardwaru počítače/serveru
VMware	Produkt, který zajišťuje virtualizaci jednoho nebo více počítačů na jednom hostitelském počítači
SLA	Dohoda o úrovni služeb
VLAN	Virtuální místní počítačová síť, slouží k logickému rozdělení počítačové sítě
CMDB	Konfigurační databáze, úložiště dat používané pro záznam atributů konfiguračních položek provozního prostředí a vztahů mezi konfiguračními položkami po celou dobu jejich životního cyklu

1.2 Seznam příloh

Číslo	Název
1	Dokumentace v jednotlivých fázích projektu
2	Architektonické principy MV k 19. 11. 2015 (jedná se o odkaz, není fyzicky přílohou)
3	Bezpečnostní politika informací MD včetně příloh (jedná se o odkaz, není fyzicky přílohou)

ČLÁNEK 2 PŮSOBNOST

2.1 Toto nařízení je vydáváno v souladu s Článkem 10 Služebního předpisu č. 18 státního tajemníka Ministerstva dopravy ze dne 20. prosince 2018 Organizační řád.

2.2 Tyto architektonické principy navazují na požadavky vyplývající z právních předpisů a na architektonické principy stanovované MV. Jsou závazné pro zadavatele a dodavatele IS MD, a to jak IS tvořených pro MD zcela na klíč (např. Registr silničních vozidel, Centrální registr řidičů aj.), tak těch částí IS, které se specificky pro MD vytvářejí nad obecně vytvořenými a více uživateli sdílenými částmi IS (např. ekonomický systém, personální systém aj.). Při výběru IS, které jsou upravovány pro potřeby MD doplňováním speciálně napsaných částí, by Architektonické principy MD měly být rovněž zohledňovány v míře ekonomicky odůvodnitelné; článek 6 se uplatní obdobně.

2.3 Tvorba a provoz IS MD musí vycházet z právních předpisů, přijaté informační koncepce MD a BPI MD (resp. jejich relevantních částí). Obecné principy IS MD jsou převzaty z požadavků MV, a to jsou:

- dostupnost,
- použitelnost,
- důvěryhodnost,
- transparentnost,
- bezpečnost,
- spolupráce a sdílení,
- udržitelnost,
- technologická neutralita,
- integrita (tzn. provoz systému garantuje integritu dat; není však uváděn ve výše citovaných požadavcích MV k datu vydání tohoto dokumentu).

2.4 Podrobnosti/výklad lze nalézt na stránkách www.mvcr.cz[1]. Architektonické principy požadované MV k 19. 11. 2015 jsou pro uvedeny v příloze, vždy je však nutno pracovat s aktuální verzí publikovanou MV na webových stránkách.

ČLÁNEK 3 ARCHITEKTONICKÉ PRINCIPY PRO DODAVATELE/ PROVOZOVATELE INFORMAČNÍCH SYSTÉMŮ MD

3.1 Dodavatelé IS MD jsou povinni se řídit následujícími architektonickými principy.

3.2 Architektonické principy pro tvorbu IS

[1] Konkrétní odkaz v době tvorby tohoto dokumentu: http://www.mvcr.cz/soubor/architektonicke-principy-vs-cr.aspx

a) **Využívat výlučně architekturu „tenkého klienta“**, tj. navrhovat a realizovat IS výhradně tak, aby na straně pracovní stanice uživatele nebylo nutno instalovat žádný pro IS speciálně vytvořený software (preferovaným klientem je standardní webový prohlížeč).
b) **Využívat důsledně vrstvené architektury**, tzn. například při komunikaci s operačním systémem nebo databází lze využívat pouze standardizovaných rozhraní a standardní komunikační protokoly dle RFC.
c) **Dokumentace IS musí být komplexní a úplná a musí umožnit instalaci a konfiguraci IS třetí stranou.**
d) **IS nesmí vyžadovat pro svůj provoz administrátorská práva k produkčnímu prostředí** serverů a dalšího hardware, virtualizační platformy, operačních systémů a databází; datový model nesmí být dynamicky měněn.
e) **Plně oddělit kód IS a data IS**, tj. v kódu IS nesmí být žádné uživatelsky definované konstanty/parametry, odkazy na externí zdroje (např. důvěryhodné certifikační autority) atp. Veškeré možnosti změny nastavení musí být realizovatelné konfiguračně (s autentizací, autorizací i logováním) bez potřeby zásahu do kódu IS.
f) **Použití jen tzv. uzavřených číselníků/roletek** (položka "ostatní" jen v odůvodněných případech), tzn. koncový uživatel nesmí mít možnost „volně“ tvořit obsah číselníků. Jedná se především o číselníky/roletky, které umožňují vkládat data, podle kterých se následně třídí, vybírají nebo párují informace. Změna (doplnění, odmazání apod.) číselníků musí být realizovatelná konfiguračně (s autentizací, autorizací i logováním) bez potřeby zásahu do kódu IS; ideálně jako samostatně přidělitelné oprávnění či role v IS (superuživatel).
g) **Zdrojový kód IS musí obsahovat komentáře v relaci s programátorskou dokumentací** minimálně ke každé použité funkci/proceduře/třídě/komponentě na takové úrovni, která umožní orientaci, porozumění kódu a jeho úpravy programátorům, kteří se na vývoji IS nepodíleli.
h) V průběhu přípravy tvorby resp. změny IS bude vytvořen a ze strany Objednatele (věcný odbor MD) schválen procesní model fungování zamýšleného IS resp. části IS po změně, který bude obsahovat minimálně popis případů použití, rámcový návrh obrazovek (wireframe) a logický datový model. Procesní model musí být schválen Objednatelem ještě před zahájením programování.
i) Data musí být ukládána výhradně v databázích (případně do filesystému) ve struktuře odpovídající datovému modelu a musí být možné jednotlivé datové položky vyhledat a přečíst prostředky databáze (resp. operačního systému), tj. bez nutnosti použít vlastní IS. Přímý přístup do databáze (resp. k filesystému s daty) smí být povolen administrátorovi pro každý jednotlivý případ na základě schválení Manažerem KB.
j) Komunikace s jinými IS musí být realizována pomocí webových služeb (web services) s popisem funkcí, vstupů a výstupů v jazyce WSDL.
k) Pro komunikaci přes HTTP smí být povoleny pouze nezbytné HTTP metody. Povolené nevyužité metody (např. zapnutí trace) představují zranitelnost a mohou způsobovat nežádoucí účinky (např. při útoku na server) a proto jejich použití musí být omezeno. IS musí splňovat RFC a další definované standardy (např. vyplnění hlaviček včetně flagů, nastavení cookies apod.)
l) IS smí k síťové komunikaci využívat pouze statických portů (na serverové straně) TCP nebo UDP portů (dynamické porty na straně serveru neumožňují nakonfigurovat firewall). K síťové komunikaci je možné použít IPv4 i IPv6 (obě alternativy bez nutnosti zásahu do IS).
m) IS musí umožňovat komunikaci s uživateli přes proxy server.

n) Kryptografické prostředky používané IS musí být konfigurovatelné bez zásahu do kódu IS. Změna kryptografických algoritmů, funkcí a délek klíčů musí být možná bez nutnosti programování v IS.

3.3 Architektonické principy pro provoz IS

a) IS musí být možné variantně provozovat na fyzických serverech a na virtuálních serverech pod Hyper-V a VMware.
b) U použitých technologických komponent jsou v maximální možné míře odstraněny veškeré části, které nejsou nezbytné pro jejich fungování (nejsou instalovány nepotřebné komponenty, aplikační SW, v prostředí nejsou uloženy zdrojové kódy). Instalovány smí být pouze komponenty nezbytné pro provoz, správu a dohled IS.
c) Zajištění provozu a dostupnosti IS a řešení provozních incidentů je definováno v SLA (včetně vyhodnocovacích metrik), který je součástí smlouvy o provozu IS.
d) Musí být definovány postupy a časová okna pro údržbu IS a změnové řízení (patch management, release management).

3.4 Architektonické principy pro bezpečnost IS

a) IS musí dodržet/naplnit všechna (relevantní) ustanovení platné BPI MD.
b) IS musí zajistit veškeré logování své činnosti minimálně v rozsahu stanoveném zákonem č. 181/2014 Sb. ve znění prováděcích předpisů.
c) IS musí umožnit zasílání veškerých logů do systémů třetích stran (např. SIEM).
d) Umožnit monitoring chování IS včetně možnosti vyhodnocování systémy třetích stran (např. napojení na centrální dohledový systém).
e) Při navazování komunikace mezi jednotlivými moduly IS s různou úrovní ohrožení se vždy navazuje komunikace z modulu s vyšším stupněm ohrožení směrem k modulu s nižším stupněm ohrožení. Obrácená komunikace vyvolaná méně ohroženým modulem se provádí přes vyzvednutí požadavku na komunikaci více ohroženým modulem. Úroveň ohrožení modulu se posuzuje na základě analýzy bezpečnostních rizik.
f) IS nezobrazuje uživatelům v chybových hlášeních žádné údaje, které by mohly být využity k narušení bezpečnosti (interní adresy, údaje o účtech, jiných uživatelích, ladicí informace a trasování, interní adresy atd.). Hláška chyby musí být taková, aby správce IS poznal jednoznačně specifické okolnosti chyby (potřebné detaily pak musí být dohledatelné v logu), nikoliv aby uživatel obdržel několik stran pro něj nesrozumitelných informací a musel je poskytovat k řízení incidentů.
g) IS kontroluje veškeré své vstupní údaje (včetně URL, cookies, HTTP hlaviček atd.). Ověřuje přípustný rozsah dat, kódování vstupních údajů, délku vstupních údajů a jiné relevantní charakteristiky, které by ho mohly dostat do nestandardního stavu. Zajistí v maximální možné míře, že se nedostanou nebezpečná nebo nekorektní data do zpracování. IS kontroluje veškerá výstupní data a nepovolí výstup dat, která by mohla ohrožovat jiné systémy.
h) IS nedovolí přístup bez autentizace k jakékoli funkci, která autentizaci má vyžadovat (např. přímý přístup při zadání celého URL není možný). Důležité IS (rozhodnutí Architekta KB) musí mít implementovánu dvoufaktorovou autentizaci.
i) U důležitých IS (rozhodnutí Architekta KB) se při přihlášení zobrazuje uživateli informace o čase předcházejícího úspěšného přihlášení a čase posledního neúspěšného pokusu o přihlášení. IS na vyžádání zobrazí uživateli historii úspěšných přihlášení a neúspěšných pokusů o přihlášení. IS musí mít možnost zakázat vícenásobné současné přihlášení téhož uživatele.
j) IS provádí reautentizaci uživatele po určité době nečinnosti. Tato doba je konfigurovatelná a pro důležité IS (rozhodnutí Architekta KB) může být odlišná

pro různé kategorie (kombinace rolí) uživatelů (např. editor a čtenář). IS odhlásí uživatele po určité době nečinnosti. Tato doba je konfigurovatelná a pro důležité IS (rozhodnutí Architekta KB) může být odlišná pro různé kategorie (kombinace rolí) uživatelů.

k) Autorizace, povolující uživateli oprávnění k operacím, se provádí vůči jeho roli v IS. IS provádí autorizační omezení přístupu uživatele při každém provádění jakékoli operace či skupiny operací. Pravidlo se neaplikuje na veřejně přístupné operace, kde není potřeba oprávnění k přístupu na operace rozlišovat.

3.5 Architektonické principy pro dokumentaci a eliminaci „vendor lock"

a) IS je/bude implementován do prostředí (operační systémy, databázové stroje, autentizační mechanismy apod.), které je již MD dominantně využíváno.
b) Dodavatel pro vývoj a provoz využije pouze prostředky, které mají zajištěnu dlouhodobou podporu výrobce spolu s perspektivou rozvoje produktu výrobcem.
c) Testovací a provozní prostředí IS (hardware, software) schvaluje (resp. definuje) Objednatel. Schválení Objednatele podléhá i jakékoliv další prostředí (včetně vývojového), pokud se v něm vyskytují data MD (včetně dat anonymizovaných či pseudonymizovaných).
d) Dokumentace musí být zpracována podle právních předpisů, pravidel OHA MV (viz webové stránky www.mvcr.cz) a interních požadavků MD na dokumentaci, které jsou uvedeny v Příloze č. 1 tohoto nařízení.
e) Dokumentace musí obsahovat minimálně:
   - datový model,
   - uživatelskou dokumentaci (včetně školicí),
   - programátorskou dokumentaci,
   - okomentovaný kompletní zdrojový kód IS,
   - administrátorskou dokumentaci včetně instalačního manuálu,
   - externí knihovny, resp. kódy třetích stran, nezbytné k funkčnímu sestavení IS,
   - skripty pro sestavení IS (jsou-li použity),
   - bezpečnostní dokumentaci včetně havarijních plánů a plánů obnovy,
   - hesla a šifrovací klíče (jsou-li použity),
   - Roll-aut plán/Exit strategii,
   - provozní deník.
f) IS musí obsahovat uživatelskou dokumentaci on-line dostupnou na obrazovkách.
g) IS musí obsahovat tzv. „info-proužek" umožňující z centrálního pracoviště provozovatele IS informovat uživatele stručným sdělením v průběhu užívání IS, aniž by činnost uživatelů tímto sdělením přerušovala.
h) Součástí dodávky a její ceny musí být komplexní licenční, resp. další práva k užívání a úpravám dodaných kódů a dokumentací k časově a teritoriálně neomezenému užití (včetně možnosti postoupit je pro účely úprav a rozvoje třetím stranám). Tato práva se musejí týkat i rozvoje dodaného IS.

ČLÁNEK 4 ARCHITEKTONICKÉ PRINCIPY PRO PROVOZOVATELE INFRASTRUKTURY

4.1 Architektonické principy pro vývojové, testovací a provozní prostředí

a) Využívat preferovaně dedikované (privátní) cloudy fyzicky umístěné v ČR.
b) Oddělené zdroje a monitoring jednotlivých provozovaných IS (alespoň virtuálně).
c) Oddělená správa/administrace zdrojů a monitoringu jednotlivých provozovaných IS.

d) Dodavatel/provozovatel využije pouze prostředky, které mají zajištěnu dlouhodobou podporu výrobce spolu s perspektivou rozvoje produktu výrobcem.
e) Dodavatel/provozovatel realizuje prostředí na škálovatelných produktech s možností flexibilní a bezpečné změny (tj. bez nutnosti reinstalace IS, realizovatelné v definovaných maintenance oknech apod.).
f) Testovací a provozní prostředí (hardware, software) schvaluje (resp. definuje) Objednatel. Schválení Objednatele podléhá i jakékoliv další prostředí (včetně vývojového), pokud se v něm vyskytují data MD (včetně dat anonymizovaných či pseudonymizovaných).
g) Testovací a produkční (a všechna další) prostředí musí být oddělena minimálně na úrovni (virtuálních) serverů i sítě (VLAN, IP).

4.2 Architektonické principy pro provoz infrastruktury

a) Dodavatel musí udržovat aktuální CMDB.
b) U použitých standardních technologických komponent jsou v maximální možné míře odstraněny veškeré části, které nejsou nezbytné pro jejich fungování (nejsou instalovány nepotřebné komponenty, aplikační SW, v prostředí nejsou uloženy zdrojové kódy). Smí být instalovány pouze komponenty nezbytné pro provoz, správu a dohledy IS/infrastruktury.
c) Zajištění provozu a dostupnosti infrastruktury a řešení provozních incidentů je definováno v SLA (včetně vyhodnocovacích metrik), který je součástí smlouvy o provozu prostředí.
d) Musí být definovány postupy a časová okna pro údržbu prostředí a změnové řízení (Patch Management, Release Management).

4.3 Architektonické principy pro dokumentaci infrastruktury

a) Dokumentace musí být zpracována podle právních předpisů, pravidel OHA MV (viz webové stránky www.mvcr.cz) a interních požadavků MD na dokumentaci, které jsou uvedeny v Příloze č. 1 tohoto nařízení.
b) Dokumentace musí obsahovat minimálně:
   - datový model včetně popisu umístění dat,
   - administrátorskou dokumentaci včetně instalačního manuálu,
   - bezpečnostní dokumentaci včetně havarijních plánů a plánů obnovy,
   - seznam a popis HW a SW prvků včetně popisu/schématu jejich propojení,
   - konfiguraci a typ použitého HW a SW,
   - hesla a šifrovací klíče (jsou-li použity),
   - informace o licenčních pravidlech použitého SW,
   - Roll-aut plán/Exit strategii,
   - provozní deník.

4.4 Architektonické principy pro bezpečnost infrastruktury

a) Infrastruktura musí dodržet/naplnit všechna (relevantní) ustanovení platné BPI MD.
b) Infrastruktura musí zajistit veškeré logování své činnosti minimálně v rozsahu stanoveném zákonem č. 181/2014 Sb. ve znění prováděcích předpisů.
c) Prvky infrastruktury musí umožnit zasílání logů do systémů třetích stran (např. SIEM).
d) Umožnit monitoring chování infrastruktury a provozovaných IS včetně možnosti vyhodnocování systémy třetích stran (např. napojení na centrální dohledový systém).

e) Zálohy dat jsou ukládány jinde než na produkčním serveru a pro důležité IS (rozhodnutí Architekta KB) i v jiné lokalitě. Funkčnost obnovy ze záloh musí být pravidelně kontrolována/ověřována.
f) Záznamy o provozu (logy) jsou ukládány pro důležité IS (rozhodnutí Architekta KB) na jiném serveru / zařízení s vlastním operačním systémem, než na kterém jsou záznamy vytvářeny.
g) Testovací, provozní i jakékoliv další prostředí (včetně vývojového), pokud se v něm vyskytují data MD (včetně dat anonymizovaných či pseudonymizovaných), musí být od veřejných i jiných (včetně prostředí pro provoz jiných IS) datových sítí odděleno minimálně jedním firewallem dozorováno IPS.

ČLÁNEK 5 ARCHITEKTONICKÉ PRINCIPY PRO DODAVATELE/PROVOZOVATELE HELPDESKU

5.1 Architektonické principy pro integrace HelpDesku

a) Pro podporu uživatelů musí mít každý IS MD implementován HelpDesk, který zajistí podporu a evidenci průběhu řešení požadavků uživatelů a incidentů v rámci L1 (základní úroveň podpory), L2 (úroveň s hlubší technickou znalostí systému) a L3 (expertní znalost systému) podpory. V rámci implementace IS je nutné přesně stanovit, kdo bude zajišťovat jednotlivé úrovně podpory, jak budou tyto úrovně spolupracovat a jak bude měřena doba řešení.
b) HelpDesk musí podporovat měření kvality dodavatelem poskytovaných služeb (SLA), včetně reportovacích nástrojů.
c) Pokud se tak MD s dodavatelem dohodne, může dodavatel provozovat vlastní HelpDesk s tím, že do centrálního HelpDesku MD musejí být zasílány veškeré incidenty a informace, které mají vazbu na výše uvedené měření kvality služeb a reportování míry dodržování dohodnutých parametrů kvality služeb (SLA).

5.2 Architektonické principy pro dokumentaci HelpDesku

a) Dokumentace HelpDesku musí splňovat všechny požadavky na IS provozované na MD.
b) Dokumentace provozu/činnosti HelpDesku (může být realizováno např. funkčností aplikace HelpDesku) musí obsahovat úplný průběh řešení požadavku včetně časových záznamů.

ČLÁNEK 6 VÝJIMKY

6.1 Dodavatel může žádat o výjimky z těchto Architektonických principů MD. Výjimky musí dodavatel písemně zdůvodnit (včetně doby trvání výjimky), předložit a požádat o stanoviska Manažera a Architekta KB na odboru ICT (O330). O povolení výjimky, resp. o podmínkách, za kterých je výjimku možno akceptovat, rozhoduje ředitel Odboru ICT MD (O330) na základě výše uvedených stanovisek.

6.2 V případě žádosti o výjimku z ustanovení odkazovaných dokumentů je nutné žádat dle jimi definovaných procesů a o podání takové žádosti informovat ředitele Odboru ICT MD (O330).

ČLÁNEK 7 ZMĚNY INFORMAČNÍCH SYSTÉMŮ MD

7.1 Pokud Dodavatel předkládá MD návrh na změnu IS, která podléhá schválení OHA MV, musí si předem vyžádat stanovisko Manažera KB MD.

7.2 Manažer KB si může po realizaci vyžádat doložení splnění podmínek; nesplnění těchto podmínek může být překážkou v akceptaci, resp. důvodem k neakceptaci dodávky/řešení.

ČLÁNEK 8 PŘECHODNÁ USTANOVENÍ

8.1 Architektura je stanovována jako dlouhodobá, cílová. Pro stávající IS MD platí komplexně pouze v případě zásadní změny IS. Pokud budou prováděny úpravy, je nutné ji použít rovněž, avšak s promítnutím výjimek plynoucích z principu finanční a časové přiměřenosti. Prohlášení o stavu plnění architektonických principů však musí být součástí všech akceptačních protokolů.

ČLÁNEK 9 REVIZE NAŘÍZENÍ

9.1 Revize nařízení se provádí povinně v těchto případech:

a) V rámci aktualizace došlo ke změnám v BPI MD.
b) Byl zjištěn nesoulad s požadavky OHA MV.
c) V rámci řešení incidentu byl identifikován nedostatek v oblasti architektury IS MD.

9.2 V případě, že jsou činnosti uvedené v tomto nařízení upraveny zvláštním právním předpisem, postupuje se podle tohoto předpisu.

ČLÁNEK 10 ZRUŠOVACÍ USTANOVENÍ

10.1 Zrušuje se Nařízení ředitele odboru ICT č.j. 1/2018-330-RDK/1 ze dne 21. prosince 2018 „Architektonické principy Ministerstva dopravy".

ČLÁNEK 11 ÚČINNOST

11.1 Toto nařízení nabývá účinnosti dnem 22. ledna 2019

[redacted]

Dokumentace v jednotlivých fázích projektů

Tento dokument je součástí metodiky řízení projektů, protože tvorba dokumentace probíhá postupně v rámci životního cyklu projektu. Níže je pak popsáno, který dokument by měl v jaké etapě projektu vzniknout a co by mělo být jeho obsahem.

I. etapa (návrh):

Projektové dokumenty podle rozhodnutí vedoucího projektu nebo zvoleného standardu (např. Základní dokument projektu, Plán projektu, Metodika vedení projektu, zápisy, Katalog rizik, Změnové požadavky)

II. etapa (vývoj):

Školicí příručka, Uživatelská příručka, Instalační příručka, Administrátorská příručka, Systémová dokumentace a Vývojová dokumentace.

III. etapa (Pilotní provoz):

Provozní dokumentace (katalogové listy, způsob zajištění provozní podpory, způsob zajištění podpory uživatelů, způsob měření SLA, provozní deník), projektové dokumenty (především pak zápisy a změnové požadavky, které vzniknou v rámci Pilotního provozu), Závěrečná zpráva/Vyhodnocení Pilotního provozu.

IV. etapa (příprava produkčního provozu):

Aktualizace provozní dokumentace a veškerých dokumentů v návaznosti na změny, provedené v průběhu Pilotního provozu.

V. etapa (podpora nebo zajištění produkčního provozu):

Aktualizace veškerých dokumentů v návaznosti na změny, provedené v průběhu laděním/optimalizace systému).

Poznámky:

1. Projektové dokumenty (Základní dokument projektu, Prováděcí projekt, Závěrečná zpráva/Vyhodnocení Pilotního provozu) se řídí pravidly projektového řízení. Veškeré požadované dokumenty musejí být smluvně zajištěny buď odkazem na příslušný standard, nebo explicitně ve smlouvě.

2. Všechny požadované dokumenty je nutné zahrnout explicitně do smlouvy (stačí odkaz na standard, pokud existuje) a případně v ní ještě detailněji upřesnit obsahovou stránku.

3. Bezpečnostní dokumentace vychází z BPI MD a může být součástí (jednou z kapitol) Administrátorské příručky – viz výše. Schvaluje ji Manažer KB.

4. Upřesnění k dokumentům, jejichž obsahová stránka není podrobněji specifikována v Release Managementu:

Školící příručka (odpovídá dodavatel)

Slouží pro provádění školení „běžných" uživatelů, klíčových uživatelů a administrátorů.

Uživatelská příručka (odpovídá dodavatel)

Obsahuje návod práce se systémem, včetně popisu scénářů použití (jak co udělám), menu, obrazovek, chybových stavů.

Instalační příručka (odpovídá dodavatel)

Je rozdělena do několika oblastí, přičemž odkazy mezi jednotlivými dokumenty jsou případně prováděny v části prerekvizity instalace:

1) databáze
   a. popis instalačního balíku, jednoznačná identifikace, obsah
   b. prerekvizity instalace
   c. instalace
      - postup instalace
      - kontrola logů
      - chybové stavy
      - adresářová/DB struktura instalace (kde se co po instalaci nachází)

2) aplikační vrstva (může být rozdělena do částí: webové služby, tenký klient, workflow, plánované úlohy, každá pak obsahuje níže uvedené části)
   a. popis instalačního balíku, jednoznačná identifikace, obsah, popis adresářů pro instalaci
   b. prerekvizity instalace
      - konfigurace bezpečnostních mechanismů (včetně hesel a šifrovacích klíčů)
      - konfigurace sítě
      - další...
   c. instalace
      - postup instalace, kontrola logů, chybové stavy, adresářová struktura instalace (kde se co po instalaci nachází)
   d. konfigurace
      - popis konfiguračních souborů a významu parametrů včetně požadovaného nastavení
   e. konfigurace dohledu a monitoringu
3) klient
   a. popis instalačního balíku, jednoznačná identifikace, co klient obsahuje, popis adresářů pro instalaci
   b. prerekvizity instalace
   c. instalace

- postup instalace, kontrola logů, chybové stavy, adresářová struktura instalace (kde se co po instalaci nachází)

d. konfigurace
   - popis konfiguračních souborů a významu parametrů včetně požadovaného nastavení

Administrátorská příručka (odpovídá dodavatel)

Na jejím základě musí být administrátor schopen provádět veškeré činnosti, které jsou nutné pro řádný chod IS včetně zálohování. Zároveň musí obsahovat metodiku pro zjištění, že je IS nefunkční. Akceptuje ji oddělení projektového řízení.

1) obecné informace o fungování IS
2) databáze
   a. seznam a popis pravidelně prováděných činností
   b. popis využití volání funkcí DB stroje
   c. popis bezpečnostních funkcí a způsobu jejich aplikace
   d. popis log souborů a způsob jejich vyhodnocování
   e. popis chybových stavů a jejich náprava
3) aplikační vrstva
   a. seznam a popis pravidelně prováděných činností
   b. popis využití a volání systémových zdrojů
   c. popis bezpečnostních funkcí a způsobu jejich aplikace
   d. popis log souborů a způsob jejich vyhodnocování
   e. popis chybových stavů a jejich náprava
   f. popis číselníků a jejich význam
4) klient
   a. seznam a popis pravidelně prováděných činností
   b. popis bezpečnostních funkcí a způsobu jejich aplikace
   c. popis log souborů a způsob jejich vyhodnocování
   d. popis chybových stavů a jejich náprava.

Systémová dokumentace (odpovídá dodavatel)

Obsahuje popis fungování systému (resp. jeho jednotlivých modulů) včetně vazeb a způsobu jeho zasazení do IS MD. Je vytvořena zejména pro potřeby integrace s jinými IS. Proto musí obsahovat nejen popis „logiky fungování" IS, ale i popis rozhraní, chybových kódů s opravnými postupy, metody a postupy škálovatelnosti výkonu a popis log souborů včetně metodiky jejich vyhodnocení. Zároveň musí splňovat požadavky, dané architekturou/ architektonickými principy.

Je určena zejména pro oddělení provozu, jehož vedoucí ji také akceptuje:
1) popis funkce a logiky IS včetně návrhu začlenění do stávajícího systému
2) seznam a popis rozhraní
3) seznam využívaných rozhraní jiných IS
4) popis toku a objemů dat
5) požadavky na změny a nastavení spolupracujících IS

6) bezpečnost (resp. bezpečnostní model – popis autentizačních a autorizačních mechanismů; definice rolí; popis bezpečnostní architektury (oddělení modulů IS, předávání dat mezi moduly, ...); ochrana komunikace; popis logování apod.)
7) licenční podmínky

Vývojová dokumentace (odpovídá dodavatel)

Poskytuje veškeré potřebné podklady pro další rozvoj a údržbu systému. Musí proto obsahovat popis architektury (v souladu s požadavky OHA MV) a veškeré analytické dokumenty, tedy:

1) popis stavových diagramů s datovými toky (event - flow diagram)
2) namapování aplikačních objektů na logický datový model
3) namapování logického datového modelu na fyzický datový model
4) podrobná programátorská dokumentace (jednotnou formou komentovaného kódu podle požadavků architektury)

Konkrétní rozsah Vývojové dokumentace může pro daný projekt upřesnit oddělení projektového řízení, které ji také akceptuje.

Provozní dokumentace (odpovídají administrátoři IS)

Dokumentuje průběh produkčního provozu, specifická nastavení konkrétní implementace a veškeré provozní zásahy, tedy:

1) seznam a popis HW prvků včetně popisu/schématu jejich propojení
2) seznam a popis SW prvků včetně popisu/schématu jejich propojení
3) konfigurace a typ použitého HW
4) konfigurace a verze použitého SW (včetně informace o licenčních pravidlech)
5) popis rozmístění dat
6) dokumentace specifických nastavení (např. zálohování, politik pro řízení přístupu apod.)
7) provozní deník - dokumentace veškerých provozních zásahů a úprav (např. změny nastavení, instalace bezpečnostních i jiných oprav operačního systému, databáze či aplikační vrstvy)
8) dokumentace průběžně prováděných testů (např. test funkčnosti záloh)
9) dokumentace změn v prostředí IS a podpůrných systémů (např. změny v antiviru, dohledový systém apod.)
10) havarijní plány a plány obnovy

Příloha č. 4

Pravidla pro provozovatele IS

OBSAH

ČÁST I. ÚVODNÍ USTANOVENÍ

Kapitola 1 DEFINICE POJMŮ A ZKRATEK

Administrátor: zaměstnanec pověřený provozovatelem IS správou a provozem svěřeného informačního systému nebo zařízení ICT infrastruktury.

DMZ: demilitarizovaná zóna (speciální typ počítačové sítě, která se využívá ke zvýšení bezpečnosti komunikace s vnějším prostředím a plní roli firewallu).

HelpDesk: kontaktní místo pro všechny uživatele IS MD pro případ potíží nebo požadavků.

IDS: Intrusion Detection System (systém detekce průniků do IS).

Informační aktivum: jakákoli informace nebo prostředek pro práci s ní, který má pro MD nějakou hodnotu.

Informační systém (IS): informační infrastruktura, soustava aplikací, organizačních opatření, procedur a souvisejících služeb pro tvorbu, získávání, zpracování, ukládání a prezentaci informací.

Incident: jakákoli odchylka od popsaného stavu, resp. výpadek služby.

IPS: Intrusion Prevention System (systém prevence průniků do IS).

Bezpečnostní incident: událost v IS, která způsobila narušení důvěrnosti, integrity, dostupnosti nebo neodmítnutelnosti informace v důsledku selhání bezpečnostních opatření nebo porušení bezpečnostní politiky.

OTP: jednorázové heslo (One Time Password).

Podpůrné informační aktivum: technické informační aktivum, zaměstnanci a dodavatelé, podílející se na provozu, rozvoji, správě nebo bezpečnosti IS.

Provozovatel IS: subjekt, zajišťující provoz daného IS tak, aby odpovídajícím způsobem a se stanovenou spolehlivostí podporoval procesy MD (provozovatelem interních IS MD je Odbor ICT).

SIEM: (Security Information and Event Management) systém pro automatickou korelaci „podezřelých událostí", jejich vyhodnocování a reporting.

Správce IS: vedoucí zaměstnanec, který určuje účel zpracování informací a podmínky provozování IS.

Technické informační aktivum: fyzická informační aktiva (především hardware ICT), programová informační aktiva (především aplikační a databázový SW), telekomunikační a další technické a podpůrné služby.

Vlastník (garant) informačního aktiva: vedoucí zaměstnanec, který odpovídá za zajištění rozvoje, použití a bezpečnosti informačního aktiva.

Kapitola 2 ROZSAH PŮSOBNOSTI

Tato příloha BPI MD stanovuje základní pravidla, zásady a principy pro provozovatele (resp. administrátorů a jejich nadřízených) IS MD. Externí subjekty jsou zavázány k plnění této přílohy smluvně.

ČÁST II. ORGANIZACE BEZPEČNOSTI INFORMACÍ

Kapitola 1 ROLE, ODPOVĚDNOSTI A PRAVOMOCI

Ředitel Odboru ICT:

- řídí dokumentaci infrastruktury ICT,
- definuje pravidla pro evidenci informačních aktiv v rozsahu služeb, poskytovaných Odborem ICT,
- definuje pravidla pro dokumentaci služeb IS MD včetně zálohování,
- zajišťuje implementaci a monitorování bezpečnostních opatření v rozsahu služeb, poskytovaných Odborem ICT,
- řídí rizika služeb, poskytovaných Odborem ICT,
- řídí technické zranitelnosti,
- vede a průběžně aktualizuje seznam bezpečnostních výjimek v souladu s požadavky přílohy č. 6 BPI MD.

Administrátor (není podstatné, zda se jedná o zaměstnance MD nebo externího subjektu):

- průběžně aktualizuje evidenci svěřených informačních aktiv v souladu s BPI MD,
- zajišťuje zabezpečení všech svěřených informačních aktiv v souladu s BPI MD,
- předchází vzniku bezpečnostních incidentů a problémů a aktivně postupuje při oznamování, odhalování a likvidaci jejich následků,
- spolupracuje při analýzách rizik, hodnocení stavu informační bezpečnosti a při bezpečnostních auditech,
- spolupracuje při zavádění a realizaci bezpečnostních opatření,
- spolupracuje při zajištění kontinuity činností a plánů obnovy po havárii,
- spolupracuje při provádění bezpečnostních auditů, analýz zranitelností a penetračních testů.

Kapitola 3 ODDĚLENÍ POVINNOSTÍ

Provozovatel zajistí dodržování pravidla neslučitelnosti provozních, bezpečnostních a kontrolních rolí. Dále zajistí, aby:

- pracovníci vývoje nebyli oprávněni provádět administraci provozních serverů, které byly předány do správy provozovatele IS,
- administrátoři neměli oprávnění umožňující editaci vzdálených auditních záznamů (logů),
- administrátoři neměli oprávnění umožňující manipulaci s daty na spravovaných zařízeních, pokud tato oprávnění nepotřebují k plnění svých pracovních povinností (pracovní povinností je míněn i zásah provedený na zdokumentovanou žádost vlastníka informačního aktiva) nebo neexistuje možnost oddělení těchto práv vzhledem k architektuře systému,
- administrátoři neměli administrátorská oprávnění k zařízením, která nespravují a nenesou za jejich provoz odpovědnost,
- administrátoři nemohli používat privilegovaný účet pro jinou než administrátorskou činnost s výjimkou účtů pro správu koncových stanic,
- veškeré účty umožňující přístup do systému byly vedeny na konkrétní osobu, nikoliv na roli.

Kapitola 4 VÝJIMKY Z USTANOVENÝCH PRAVIDEL

Výjimky z pravidel stanovených touto přílohou BPI MD (v důsledku technického omezení, architektury systému, omezenou pracovní kapacitou nebo specifikou pracovních povinností specialistů ICT), musí být předem zdokumentovaným způsobem schváleny Manažerem KB.

ČÁST III. HODNOCENÍ PODPŮRNÝCH INFORMAČNÍCH AKTIV

Vlastník podpůrného informačního aktiva provádí jeho hodnocení. Stupeň hodnocení podpůrného informačního aktiva musí odpovídat hodnocení primárního informačního aktiva s nejvyšším stupněm hodnocení, na jehož zpracování se dané podpůrné informační aktivum podílí.

ČÁST IV. ŘÍZENÍ PŘÍSTUPU

Kapitola 1 POŽADAVKY NA ŘÍZENÍ PŘÍSTUPU

Všem uživatelům mohou být přidělena pouze taková oprávnění, která potřebují k vykonávání svých pracovních povinností. Při přidělování uživatelských práv platí zásada „co není povoleno, je zakázáno".

Administrátor je oprávněn přidělit uživateli oprávnění, pokud jsou splněny tyto podmínky:

- přidělení uživatelského oprávnění bylo schváleno správcem IS v souladu s přílohou č. 5 BPI MD,
- nastavení umožňuje jednoznačné určení zodpovědnosti za prováděné operace,
- o přidělování a využívání přístupových práv jsou vedeny auditní záznamy (logy) v souladu s požadavky této přílohy BPI MD,
- pokud jsou pro řízení přístupu použity biometrické prostředky, musí být použity v souladu s platnou legislativou.

Administrátoři jsou povinni alespoň 1x měsíčně kontrolovat přístupová oprávnění. Případné zjištěné „non-compliance" stavy (např. existence účtu zaměstnance, který již na MD nepracuje) musí administrátoři neprodleně řešit.

Součástí této kontroly musí být dále identifikace dlouhodobě nevyužívaných účtů (účet nebyl použit déle než 120 dní). Dlouhodobě nevyužívané standardní uživatelské účty musí být zrušeny, nebo dočasně zneplatněny. Možnost zrušení nebo potřebu ponechání aktivních dlouhodobě nevyužívaných technologických účtů musí administrátorovi odsouhlasit správce IS.

Pro potřeby přístupů dodavatelů za účelem podpory nebo řešení problémů (neplatí pro externisty v rolích administrátorů systémů, na ty se vztahují stejné požadavky jako na zaměstnance MD ve stejných rolích) mohou být vytvořeny účty, pomocí kterých mohou zaměstnanci dodavatele přistupovat k systémům. Tyto účty musí splňovat požadavky uvedené v ČÁSTI IV, Kapitole 3 (*„Správa a řízení přístupu uživatelů"*). Pokud je nutné vytvořit pro potřeby podpory účet, který bude sdílen více pracovníky jednoho dodavatele, musí takový účet splnit tyto podmínky:

- s dodavatelem je podepsána platná smlouva,
- jsou dodržena všechna ustanovení této přílohy BPI MD,
- účet je implicitně (defaultně) zablokován a odblokovává se pouze pro dobu nezbytnou k vyžádanému zákroku,
- uživatelské účty nesmějí být sdíleny více dodavateli.

Při konfiguraci systému musí administrátor nastavit politiku pro uživatelská hesla, která bude kontrolovat dodržování požadavků Vyhlášky o kybernetické bezpečnosti (Správa a ověřování identit).

Pokud dojde k uzamčení účtu z důvodu velkého počtu neúspěšných přihlášení, musí být účet uzamčen minimálně 30 minut nebo do zásahu administrátora.

Administrátor IS komunikujícího s Internetem a sdílejícího autentizaci s důvěryhodnými systémy ve vnitřní síti, které slouží mj. i pro autentizaci (např. AD), je povinen zajistit, že při dosažení nejvyššího povoleného počtu neúspěšných přihlášení bude pouze blokováno další přihlášení, nikoliv však uzamčení účtu na úrovni důvěryhodných autentizačních služeb ve vnitřní síti.

Je povoleno použití stejných hesel k serverům patřícím ke stejné službě a zároveň zpracovávajícím informace stejné klasifikace.

Hesla se nesmějí v systému vyskytovat v otevřené (nešifrované) podobě. Administrátoři jsou povinni používat pro šifrování hesel nejsilnější algoritmus, který je v distribuci systému dostupný, pokud to negativně neovlivní chod systému, přičemž mohou využít i silnější algoritmy dodávané mimo standardní distribuci systému.

Je-li to technicky možné, jsou administrátoři povinni umožnit (případně upřednostnit) silnou autentizaci – např. použití interních autentizačních služeb nebo jednorázových hesel zasílaných odděleným komunikačním kanálem.

V případě použití jednorázového hesla, musí být toto heslo generováno off-line (nezávisle na komunikačním kanálu použitém k přihlašování) k tomu určeným zařízením, nebo musí být uživateli doručeno bezpečným kanálem fyzicky odděleným od komunikačního kanálu použitého k přihlašování a musí splňovat následující parametry:

- maximální doba platnosti OTP od jeho vydání nebo zaslání: 5 minut, nebo vyžádání nového OTP (co nastane dříve),
- minimální délka: 11 znaků (z množiny 0-9), nebo 7 znaků (z množiny a-z + 0-9).

Kapitola 2 ŘÍZENÍ PŘÍSTUPU K SÍŤOVÝM SLUŽBÁM

Pro řízení přístupu uživatelů k pracovním stanicím musí být vytvořeny a aplikovány skupinové politiky Active Directory. Tyto politiky specifikuje Odbor ICT.

Na pracovních stanicích je zakázáno sdílet celé disky i jednotlivé adresáře kromě standardního systémového sdílení.

Na uživatelských stanicích je zakázáno sdílení tiskáren, všechny tiskárny používané více zaměstnanci musí být připojeny k lokální síti pomocí tiskového (print) serveru. Tiskárny umístěné ve společných prostorách MD (chodby, openspace a podobně) musí být vybaveny autentizačními mechanismy pro uživatele. Administrátoři jsou povinni zabezpečit funkčnost těchto mechanismů, tak aby nedocházelo ke spouštění tiskových úloh bez přítomnosti oprávněných uživatelů.

Na standardních serverech nesmí být uživatelům povoleno přihlášení k operačnímu systému. Uživatelé se mohou přihlašovat pouze ke službám, které jsou serverem nabízeny dle provozní dokumentace a stanovení účelu serveru.

K technologickým stanicím mají uživatelé zakázaný přístup, mohou k nim přistupovat pouze jejich administrátoři, případně pověření technici.

K bezpečnostním prvkům mohou přistupovat pouze jmenovitě určení administrátoři, Manažer KB, Architekt KB a případně jmenovitě pověření uživatelé.

Kapitola 3 SPRÁVA A ŘÍZENÍ PŘÍSTUPU UŽIVATELŮ

3.1 Zřízení a zrušení uživatelského účtu

Administrátoři mohou zřídit či zrušit uživatelský účet pouze na základě schváleného požadavku. Každý uživatelský účet musí mít unikátní ID v rámci systému, kde je zřízen, které odpovídá jmenné konvenci Odboru ICT.

Administrátoři jsou povinni minimálně 1x měsíčně (doporučeno je po 1. dnu v měsíci) kontrolovat přidělení přístupových oprávnění uživatelům, kteří již nejsou zaměstnanci MD, jsou dlouhodobě nepřítomni, resp. s nimi byla ukončena spolupráce jako s externisty. Pokud administrátor zjistí přidělení oprávnění takovému uživateli, musí okamžitě účet zneplatnit.

3.2 Zřízení přístupu uživatele

Administrátoři jsou oprávněni uživatelským účtům nastavit přístupová oprávnění pouze na základě schváleného požadavku.

Jakékoliv změny v nastavení přístupových oprávnění mohou administrátoři provádět pouze na základě schválených požadavků, nebo při řešení havarijních situací (je-li to nezbytné pro vyřešení situace), nebo pokud ponechání přístupových práv ohrožuje provoz nebo stabilitu systému. O změně přístupových práv, která nebyla provedena na základě schváleného požadavku nebo nebyla hlášena jako bezpečnostní incident, musí administrátoři bez zbytečného odkladu informovat dotčeného uživatele nebo jeho nadřízeného.

Je zakázáno zřizování hromadných nebo skupinových uživatelských účtů, případně sdílení těchto účtů. Takovéto účty jsou administrátoři povinni smazat nebo zakázat okamžitě při jejich detekci a jejich existenci hlásit jako bezpečnostní incident.

Přístupová oprávnění musí být definována jako vazba na pracovní pozici zaměstnance (definuje nadřízený zaměstnanec), v případě změny pracovní pozice musí administrátoři odpovídajícím způsobem změnit i přístupová oprávnění uživatelského účtu zaměstnance.

3.3 Řízení privilegovaných přístupových práv

Privilegovaný přístup k prvku IS může mít přidělen pouze pracovník, který je pověřen administrací (obdobně platí i pro účty umožňující částečnou administraci, např. backup). Seznam pracovníků s administrátorskými resp. privilegovanými oprávněními musí být součástí provozní dokumentace.

Administrátorské účty se nesmějí používat pro činnosti nesouvisející s administrací. Pro běžnou agendu musí administrátor využívat neprivilegovaného účtu, pro jednotlivý administrativní zásah je doporučeno používat příkazy pro spuštění aplikace s jinými právy, než je aktuální login ('runas' resp. 'su do'), případně bezpečné (např. „ssh") připojení ke službě vyhrazené na daném serveru pro administraci umožňující pouze lokální připojení. Toto ustanovení se nevztahuje na uživatelské účty, které mají přidělená administrátorská práva pro pracovní stanice.

Pro administraci i jakoukoliv jinou činnost je zakázáno přímé přihlašování k implicitním (defaultním) systémovým účtům určeným pro administraci. Musí být vytvořen účet pro každou fyzickou osobu provádějící administraci, která následně použije utilitu 'runas' resp. 'su do', případně použije bezpečné (např. „ssh") připojení ke službě vyhrazené na daném serveru pro administraci umožňující pouze lokální připojení.

Administrátoři jsou povinni účelně používat všechny dostupné mechanismy pro řízení přístupu (např. ACL či nastavení packet filtru na síťovém rozhraní). Pokud je to technicky možné, jsou povinni využívat přidaných hodnot trusted systémů.

Administrátoři jsou povinni využívat možnosti nastavovat práva ke zdrojům OS (např. práva zapisovat do registrů, skupina wheel u UNIXu a podobně), pokud je takové nastavení účelné.

3.4 Řízení chráněných autentizačních informací uživatelů

Všechny systémy musí, je-li to technicky možné, při prvním přihlášení uživatele vynucovat změnu prvotního hesla (=hesla, které bylo uživateli předáno správcem systému). Stejná změna hesla musí být vynucena i při každém novém vygenerování hesla (např. při zapomenutí hesla uživatelem). Předání takového hesla musí být realizováno odděleným komunikačním kanálem (např. nové heslo k webovému portálu nesmí být posláno emailem, ale může být zasláno SMSkou na mobil uvedený v oficiálním telefonním seznamu). Heslo nesmí být mezi administrátory sdíleno, musí být uchováváno v tajnosti a při předávání nesmí být dostupné třetí osobě.

Administrátor je po instalaci systému nebo síťového prvku a jakéhokoliv dalšího zařízení či softwaru vždy povinen neprodleně změnit výchozí autentizační informace výrobce.

3.5 Odpovědnost uživatelů

Odpovědnosti uživatelů jsou definovány v Příloze č. 3 BPI MD.

3.6 Řízení přístupu k systémům a aplikacím

Administrátoři jsou povinni používat netriviální hesla, jež respektují požadavky na sílu hesla stanovené v ČÁSTI IV, Kapitole 2 této přílohy BPI MD („Pravidla řízení přístupu").

Administrátoři jsou povinni chránit hesla před kompromitací a minimalizovat všechna rizika související s jejich vyzrazením.

Administrátoři jsou povinni ukládat šifrovací klíče chráněné pomocí „passphrase", pokud klíč neslouží pro automatický provoz.

Administrátoři jsou povinni, pokud je to technicky možné, zajistit běh služeb pod jinými oprávněními, než má superuživatel („root", resp. „administrator").

Administrátoři jsou povinni používat „access control" listy a další mechanismy řízení oprávnění ať už k souborovým systémům nebo k aplikacím, pokud je to účelné, a zároveň, pokud je to technicky možné, jsou povinni využívat přidaných hodnot „trusted" systémů. Administrátoři jsou povinni zajistit, aby k jimi spravovaným serverům nebylo možné přistupovat jinak, než definovaným a schváleným způsobem (např. vypnutí nepoužívaných služeb a „daemonů", využití interních firewall systémů a podobně).

U serverů, kde je to technicky možné, s uživatelskými účty, které mohou díky svému nastavení umožnit vykonání nějaké systémové úlohy, je administrátor povinen nastavit limity takovému uživateli, které omezí využití CPU, RAM, místa na disku a podobně.

Administrátoři jsou povinni zajistit monitoring přístupu a činnosti externistů v roli podpory k informačním aktivům MD – v případě vzdáleného přístupu externistů (po síti) logováním, v případě fyzického přístupu k zařízení zajištěním odborného dozoru po celou dobu zásahu.

3.7 Bezpečné postupy přihlášení

Administrátoři jsou povinni, je-li to technicky možné, implementovat takovou politiku pro přihlášení, která zajistí:

- heslo nebude při zadávání, resp. ani v jiných případech, zobrazeno,
- heslo nebude přenášeno (např. mezi uživatelským SW a serverem) v nešifrované podobě,
- informování uživatele o špatném přihlášení, které mu neposkytne žádné informace či nápovědu pro uhodnutí přihlašovacího jména či hesla (doporučujeme uvádět pouze "špatné uživatelské jméno či heslo" a kontakt na pracovníka uživatelské podpory),

- automatické odhlášení uživatele nebo uzamčení pracovní stanice po 15 minutách nečinnosti.

Administrátoři jsou povinni zajistit ochranu proti „brute force" (hrubý útok automatickým opakovaným přihlášením a podobně) a dalším technickým útokům na hesla, viz minimální požadavky na nastavení politiky pro hesla, definované v ČÁSTI IV, Kapitole 2 této části (Pravidla řízení přístupu") a požadavky na logování přístupů definované v ČÁSTI VI, Kapitole 4 této přílohy BPI MD („Monitorování").

Pro SSH autentizaci administrátorů k systémům není povoleno používání pouze jména + hesla.

3.8 Použití privilegovaných obslužných programů

Administrátoři jsou povinni zajistit, aby uživatelé mohli přistupovat ke zdrojům jimi spravovaných systémů pouze v rozsahu stanoveném schválenými přístupovými oprávněními. Zejména jsou administrátoři povinni zamezit uživatelům v přístupu k systémovým adresářům a souborům a zajistit, aby všechny uživatelem spouštěné programy pracovaly výhradně pod účtem uživatele.

3.9 Řízení přístupu ke zdrojovému kódu programu

Ke zdrojovým kódům programů mohou přistupovat pouze pracovníci pověření vývojem (případně pracovníci provádějící audit zdrojového kódu).

Zdrojový kód nesmí být umístěn na provozních serverech; zdrojový kód aktuálně testovaných aplikací může být v případě potřeby ve výjimečných případech umístěn na testovacích serverech.

Vývojáři nesmějí být zároveň administrátory provozních serverů.

ČÁST V. KRYPTOGRAFICKÁ OPATŘENÍ

Administrátoři IS, které využívají některá kryptografická opatření (algoritmy, bezpečnostní protokoly, klíčové hospodářství, speciální software a hardware), musí při jeho celém životním cyklu (od instalace, konfigurace, provozu, výroby a distribuce klíčů a jiných směnných prvků (např. tokenů pro bezpečné uložení certifikátů) až po likvidaci tohoto systému) postupovat v souladu s dodanou dokumentací a minimálními požadavky, které jsou uvedeny v této příloze BPI MD. Dále pak je vhodné brát v potaz hodnocení bezpečnosti příslušného řešení resp. další dokumenty, které se zabývají aspekty kryptografické ochrany.

Při výběru algoritmů a síly mechanismů se administrátoři řídí minimálními požadavky uvedenými v této kapitole a výsledky hodnocení a příslušnými doporučeními.

Kapitola 1 GENERÁTORY NÁHODNÝCH ČÍSEL

MD preferuje použití fyzikálního generátoru náhodných čísel. V případě provozování takovéhoto generátoru je potřeba zajistit statistické testování na kvalitu výstupu a test funkčnosti generátoru.

V případě použití pseudonáhodného generátoru (PRNG – Pseudo-Random Number Generator) náhodných čísel je potřeba zajistit vhodný nepredikovatelný způsob náhodného a dostatečně velkého počátečního nastavení („seed"). Množina všech reálně dosažitelných počátečních nastavení musí být tak velká, aby nedávala útočníkovi možnost získat výsledky takovéhoto pseudonáhodného generátoru.

Kapitola 2 SYMETRICKÉ ALGORITMY ASYMETRICKÉ ALGORITMY A HASHOVACÍ FUNKCE

Výběr šifrovacích algoritmů a hashovacích funkcí se řídí aktuálními doporučeními Národního úřadu pro kybernetickou a informační bezpečnost.

Použití jiných algoritmů a funkcí musí být schváleno jako výjimka v souladu s přílohou č. 6 BPI MD.

Kapitola 3 SPRÁVA KLÍČŮ A CERTIFIKÁTŮ

Při výběru symetrického a asymetrického algoritmu je potřeba vždy doplnit popis životního cyklu použitého klíče a jeho distribuce. Tento popis musí být v tomto minimálním rozsahu: generování klíče, uložení klíče, vlastnictví klíče, přístup ke klíči, požadavky na jeho použití (např. u symetrické šifry uvést omezení na objem šifrovaných dat), uvést, zda je možné provést obnovu klíče a pokud ano, tak za jakých podmínek, postup při kompromitaci klíče.

Za správu klíčů a certifikátů odpovídá garant certifikátu. Tj. každá dvojice klíčů asymetrické kryptografie a každý klíč symetrické kryptografie má svého garanta. Jeho povinností je:

- zajistit bezpečné uložení kopie klíče,
- podílet se na rozhodnutí, které klíče a certifikáty je možné nasadit pro určitou aplikaci,
- zajistit používání klíčů a certifikátů ve shodě s certifikační politikou vydávající certifikační autority,
- bezpečné předání klíčů správcům serverů, respektive aplikací,
- kontrolovat využívání klíčů a certifikátů,
- vést přehled, kde jsou jednotlivé klíče a certifikáty používány a komu byly předány,
- vést přehled o platnosti certifikátů a zajistit jejich včasnou obnovu,
- v případě potřeby zajistit odvolání certifikátu.

ČÁST VI. BEZPEČNOST PROVOZU

Kapitola 1 PROVOZNÍ POSTUPY A ODPOVĚDNOSTI

1.1 Dokumentace provozních postupů

Veškeré provozní postupy musí být dokumentovány. Provozní postupy musí jednoznačně popisovat všechny rutinně prováděné zásahy v IS MD. Nedílnou součástí těchto postupů jsou i plány zálohování, havarijní plány a plány obnovy systému po havárii.

Všechna zařízení v IS MD musí být (jako podpůrná informační aktiva) identifikována a evidována. Tato evidence musí být klasifikována přinejmenším bezpečnostním klasifikačním stupněm „PRO VNITŘNÍ POTŘEBU".

Evidence pracovních stanic musí obsahovat minimálně následující údaje:

- informace o HW i SW konfiguraci stanice (včetně konfigurace síťových připojení a standardních aplikací),
- informace o všech provozních aktivitách (včetně data a času a jména administrátora, který zásah provedl),
- informace o konfiguraci softwaru instalovaného nad rámec standardních instalací,
- informace o přidělení stanice konkrétnímu uživateli (včetně zdůvodnění a účelu).

Evidence serverů musí obsahovat minimálně následující údaje:

- informace o HW i SW konfiguraci serveru (včetně konfigurace síťových připojení a běžících služeb nebo "démonů"),
- informace o všech provozních aktivitách (včetně data a času a jména administrátora, který zásah provedl),
- informace o instalovaném software (aplikace, databáze ...),
- informace o požadavcích a realizaci zálohování dat i systému,
- informace o klasifikačním stupni informací, které jsou na serveru uloženy nebo zpracovávány,
- informace o konfiguraci instalovaného bezpečnostního software a nastavení auditování událostí,
- informace o fyzickém umístění,
- informace o administrátorech zodpovědných za provoz serveru i jednotlivých aplikací.

Evidence síťových prvků („huby", „switche", „routery", „firewally" ...) musí obsahovat minimálně následující údaje:

- informace o konfiguraci HW i SW zařízení včetně informací o nastavení auditování událostí,
- informace o fyzickém umístění,
- informace o všech provozních aktivitách (včetně data a času a jména administrátor, který zásah provedl),
- informace o administrátorech zodpovědných za provoz zařízení.

Součástí evidencí prvků IS musí být ke každému prvku i seznam jeho administrátorů. K těmto evidencím mohou přistupovat pouze:

- administrátoři – možnost čtení i zápisu pro záznamy o systémech, které jsou v jejich správě,
- zaměstnanci v oblasti bezpečnosti (Manažer KB a jím pověření zaměstnanci) – možnost čtení pro všechny záznamy a možnost zápisu relevantních informací (např. informace o bezpečnostních testech),
- auditoři – možnost čtení pro všechny záznamy,
- a další zaměstnanci, kteří informace potřebují ke své práci (např. HelpDesk) – přístupy definované po domluvě s administrátory daného zařízení nebo systému na základě pracovních povinností.

1.2 Řízení změn

Všechny změny, prováděné v rámci IS MD podléhají změnovému řízení. Za změny ve smyslu ustanovení této kapitoly nejsou považovány rutinní provozní zásahy.

Každé změně musí předcházet analýza jejího dopadu na provoz a musí se k ní vyjádřit administrátoři zařízení nebo systémů, kterých se dotýká. Na základě této analýzy musí realizátor změny vypracovat harmonogram, který zajistí minimalizaci výpadků jednotlivých komponent systému a jím poskytovaných služeb. Analýza dopadů i harmonogram musí být dokumentovány, kromě případů, kdy se nejedná o změny zásadního charakteru na spravovaných zařízeních – určuje administrátor. Požadovanou dokumentaci zajistí žadatel změny, ostatní pracovníci (např. administrátoři) jsou povinni poskytnout potřebné součinnosti.

Pokud změna svým rozsahem znamená zásah do podstatné části IS, dotýká se zařízení v DMZ, dotýká se zařízení nebo systémů provozujících bezpečnostní technologie, případně se dotýká zařízení zpracovávajících informace klasifikované bezpečnostním klasifikačním stupněm „CHRÁNĚNÉ", musí změnu kromě provozních útvarů odsouhlasit i Manažer KB.

1.3 Plánování kapacit

Plánování kapacit jednotlivých komponent IS je odpovědností Odboru ICT. Organizační jednotky, případně externí subjekty, odpovídají za monitorování provozu systému tak, aby zajistily včasnou detekci vzniklých problémů se zdroji (disková kapacita, operační paměť propustnost sítě a podobně). Součástí provozních doporučení je i plánování budoucí spotřeby kapacit s ohledem na plánování a řízení změn na MD. Při plánování kapacit musí být zohledněny i aplikace a systémy, které pro ukládání dat využívají externí datová úložiště (např. „cloudové" systémy).

Administrátoři musí brát při výběru software (i hardware) v úvahu počet a stav řešení známých zranitelností všech jeho verzí v historii.

1.4 Princip oddělení prostředí vývoje, testování a provozu

Vývojové, testovací a provozní prostředí musí být odděleny. Testování nových verzí software (resp. nového hardware) nesmí probíhat v provozním prostředí. Tyto testy nesmějí být prováděny nad ostrými daty. Pokud takové testování není možné, musí případné výjimky schválit administrátoři provozních zařízení, vlastnící dat a Manažer KB. Testování nad osobními údaji je možné pouze po jejich anonymizaci.

Nový hardware či software může být nasazen až poté, co jsou splněny předem definované podmínky. Tyto podmínky definují zaměstnanci Odboru ICT, případně je upřesňují pro konkrétní HW či SW a schvaluje je Manažer KB.

Na provozních serverech nesmí být instalovány překladače a systémové utility, které nejsou nezbytné pro správu.

Pracovníci vývoje nesmějí mít administrátorský přístup k provoznímu prostředí. Pokud to z technických či provozních důvodů není možné, musí případné výjimky schválit administrátoři provozních zařízení, Manažer KB a musí být navržena kompenzační opatření.

Kapitola 2 OCHRANA PŘED ŠKODLIVÝM KÓDEM

Jako ochrana proti škodlivým programům musí být instalován antivirový software s centrálním managementem. V případě potřeby mohou administrátoři instalovat i další software pro detekci škodlivého kódu. Takový software musí být schválen Manažerem KB a Odborem ICT.

Administrátorům je zakázáno vypínat bezdůvodně antivirovou ochranu. O vypnutí musí být vytvořen záznam v příslušné provozní dokumentaci. Antivirový software musí být instalován na všech uživatelských stanicích a relevantních serverech (servery s operačním systémem Windows, „fileservery", mailové „gatewaye" a další, pro které příslušné SW nástroje existují, resp. jsou přínosné).

Nastavení antivirové kontroly pro uživatele jsou administrátoři povinni konfigurovat takovým způsobem, aby ji uživatelé nemohli svévolně vypínat.

Administrátoři mohou na provozní systémy instalovat pouze software, který odpovídá požadavkům stanoveným v odstavci 5.4 („Instalace softwaru na provozní systémy").

Administrátoři odpovídají za to, že veškerý software na serverech i pracovních stanicích je instalován, konfigurován a spravován tak, aby pravděpodobnost napadení škodlivým programem byla minimalizována. To znamená zejména:

- požadování autentizace pro každé spojení se serverem či stanicí ze sítě (interní i veřejné),
- zakázání všech vzdálených spojení se servery i stanicemi, která nejsou potřebná pro výkon činnosti, dohled či správu,
- vypnutí všech voleb („features"), které nejsou potřebné pro provoz serveru či pracovní stanici, resp. pro práci uživatelů,
- bezpečné nastavení všech programů komunikujících po síti,

- pravidelná aktualizace v závislosti na nově objevených chybách a zranitelnostech.

Administrátoři jsou dále povinni provádět pravidelné kontroly jimi spravovaných zařízení na přítomnost škodlivého kódu.

Kapitola 3 ZÁLOHOVÁNÍ

Požadavky na četnost, frekvenci, dostupnost a dobu uchování záloh stanoví vlastník zpracovávaných informací v závislosti na dopadech nedostupnosti či ztráty dat. Veškeré zálohy musí podléhat obdobným ochranným opatřením jako původní data a musí být klasifikovány klasifikačním stupněm stejným nebo vyšším, jako jejich nejvýše klasifikovaná předloha.

Administrátoři zodpovědní za zálohování jsou povinni:

- zajistit dostatečnou zálohovací kapacitu,
- pravidelně (doporučeno alespoň 1x za rok) kontrolovat životnost použitých zálohovacích médií dle specifikací výrobce (média s končící životností nahradit),
- pravidelně (doporučeno alespoň 1x za rok) kontrolovat čitelnost zálohovaných dat
- pravidelně (doporučeno alespoň 1x za rok) provádět testovací obnovu dat.

Kapitola 4 MONITOROVÁNÍ

4.1 Požadavky na auditní záznamy

Administrátoři jsou povinni nastavit na spravovaných systémech logování minimálně dle požadavků této přílohy BPI MD. Pro konkrétní systémy může být správcem IS požadováno logování nad rámec této přílohy BPI MD. Každý záznam v logu musí obsahovat minimálně tyto informace:

- datum a čas, kdy k události došlo,
- ID uživatele (či automatu),
- zdroj (IP adresa, lokální konzole a podobně),
- vlastní auditní informaci.

V logovacích souborech nesmí být při chybných i úspěšných přihlášeních zaznamenáváno heslo.

Administrátoři jsou povinni při vzdáleném on-line logování zajistit zasílání definovaných (domluvených při přípravě on-line logování) záznamů v případě, že v definované době nedošlo k žádné události, která by auditní záznam vygenerovala („keep alive"); tato doba je minimálně 300 sekund, pro konkrétní systémy může být na základě klasifikace zpracovávaných informací zkrácena.

Veškeré uvažované změny v nastavení logování (vynucené např. změnami v provozu zařízení, jeho upgradem nebo nahrazením) jsou administrátoři povinni bez prodlení oznámit Manažerovi KB; v případě použití vzdáleného logování i pracovníkům odpovědným za provoz systémů pro sběr těchto logů.

V případě, že z technických (případně jiných) důvodů není možné zajistit logování podle požadavků této přílohy BPI MD, případně další řídící dokumentace, jsou administrátoři povinni tuto skutečnost ohlásit Manažerovi KB a zažádat o výjimku.

Výpadek auditních funkcí požadovaných touto přílohou BPI MD musí být řešen jako bezpečnostní incident.

4.2 Monitorování uživatelských aplikací

Všechny aplikace musí umožňovat nastavení logování v níže uvedeném rozsahu. Pro záznam auditních událostí mohou aplikace využívat prostředky operačního systému či jiného instalovaného SW.

Bezpečnostní log aplikace musí zaznamenávat úspěšné i neúspěšné události minimálně v tomto rozsahu:

- informace o přihlášení a odhlášení uživatelů i administrátorů,
- informace o změnách v metodě zabezpečení (včetně nastavení politiky pro logování),
- informace o provedených změnách dat,
- informace o přístupech uživatelů k informacím klasifikovaným stupněm „CHRÁNĚNÉ",
- informace o importech a exportech dat.

Administrátor stanoví na základě dohody s Manažerem KB pravidla a rozsah logování v závislosti na klasifikačním stupni informací, se kterými aplikace pracuje. Vlastní nastavení auditních pravidel musí být schváleno Manažerem KB nebo jím pověřenou osobou.

4.3 Monitorování uživatelských stanic

Logování musí být zapnuto na všech uživatelských stanicích. Bezpečnostní log může být dostupný (pokud to je technicky možné, tak jen pro čtení) pouze uživatelům zařazeným ve skupině „administrators" (resp. v příslušné globální skupině). Bezpečnostní log musí zaznamenávat úspěšné i neúspěšné události minimálně v tomto rozsahu:

- přihlášení a odhlášení,
- správa uživatelů a skupin,
- připojení a odpojení externích zařízení,
- změny v metodě zabezpečení,
- použití uživatelských práv.

Velikost těchto logů musí být nastavena minimálně na 16384 kB, staré události budou přepisovány novými až v případě potřeby.

Je-li na uživatelské stanici instalován jiný operační systém než standardní Windows, je jeho administrátor povinen zajistit logování událostí na úrovni popsané v této kapitole.

4.4 Monitorování standardních serverů a technologických stanic

Logování musí být zapnuto na všech serverech. Správce IS ve spolupráci s Manažerem KB stanoví pravidla a rozsah logování v závislosti na službách poskytovaných serverem.

Bezpečnostní log musí zaznamenávat úspěšné i neúspěšné události minimálně v tomto rozsahu:

- informace o přihlášení a odhlášení,
- informace o změnách v metodě zabezpečení (včetně nastavení politiky pro logování),
- připojení a odpojení externích zařízení,
- informace o změně identity („su" nebo "runas"),
- informace o spouštění a zastavování služeb nebo "démonů",
- informace o změně systémového data,
- informace o vypnutí nebo restartu systému.

4.5 Monitorování serverů v DMZ

Všechny servery v DMZ musí vzdáleně logovat události vyžadované pro logování standardních serverů a navíc také:

- informace o odmítnutých paketech z interních „packetových" filtrů,

- informace o neúspěšném přístupu ke službě z "tcp wrapperu",
- informace od procesů obsluhujících aplikační vrstvu („http", „smtp", a podobně).

Logovaná musí být minimálně IP adresa a čas přístupu, ale pokud je to možné, i další informace (např. kompletní hlavičky paketů).

Administrátor stanoví na základě dohody s Manažerem KB pravidla a rozsah logování v závislosti na službách poskytovaných serverem. Vlastní nastavení auditních pravidel musí být schváleno Manažerem KB nebo jím pověřenou osobou.

4.6 Monitorování serverů zpracovávajících „CHRÁNĚNÉ" informace

Všechny servery, které pracují s informacemi klasifikovanými bezpečnostním klasifikačním stupněm „CHRÁNĚNÉ" musí vzdáleně logovat události vyžadované pro logování standardních serverů a navíc také:

- informace o odmítnutých paketech z interních „packetových" filtrů,
- informace o neúspěšném přístupu ke službě z „tcp wrapperu",
- relevantní informace z aplikačního SW (pokud si administrátor není jist relevancí informací pro centrální logování, určí ji ve spolupráci s Manažerem KB nebo jím pověřenou osobou).

Administrátor stanoví na základě dohody s Manažerem KB pravidla a rozsah logování v závislosti na informacích zpracovávaných serverem. Vlastní nastavení auditních pravidel musí být schváleno Manažerem KB nebo jím pověřenou osobou.

4.7 Monitorování síťových prvků

Všechny síťové prvky musí logovat následující události:

- úspěšné i neúspěšné pokusy o přihlášení nebo odhlášení k síťovému prvku,
- změny v konfiguraci,
- výpadky dostupnosti zařízení a síťových tras.

4.8 Monitorování bezpečnostních zařízení

Všechny bezpečnostní prvky musí vzdáleně logovat události vyžadované pro logování standardních serverů a navíc také:

- informace o odmítnutých paketech z interních „packetových" filtrů,
- informace o neúspěšném přístupu ke službě z „tcp wrapperu",
- všechny zásahy do konfigurace i do všech dalších součástí systému (např. změny v datových souborech).

Administrátor stanoví na základě dohody s Manažerem KB pravidla a rozsah logování v závislosti na službách poskytovaných serverem. Vlastní nastavení auditních pravidel musí být schváleno Manažerem KB nebo jím pověřenou osobou.

4.9 Ochrana auditních záznamů

Administrátoři jsou povinni auditní záznamy klasifikovat dle BPI MD a dále je vzhledem ke klasifikačnímu stupni odpovídajícím způsobem chránit. Pro klasifikaci platí, že logy musí být klasifikovány přinejmenším stupněm „PRO VNITŘNÍ POTŘEBU".

Auditní záznamy jsou administrátoři povinni uchovávat minimálně po dobu jednoho roku, nebo dle ustanovení platné legislativy, pokud tato stanoví delší čas. Kratší dobu uchovávání logů lze stanovit pouze v případě vzdáleného logování událostí do centrálního systému pro sběr logů (případně SIEM), nebo výjimkou udělenou Manažerem KB nebo jím pověřenou osobou.

Administrátoři jsou povinni na vyžádání Manažera KB zajistit vzdálené logování událostí do centrálního systému pro sběr logů (SIEM) na jimi spravovaných zařízeních. Konkrétní způsob

realizace vzdáleného logování bude stanoven dle možností monitorovaného zařízení s maximalizací využití nástrojů na zařízení instalovaných.

K auditním záznamům mohou přistupovat pouze:

- administrátoři zodpovědní za provoz zařízení, které logy vytváří,
- administrátoři systému pro zpracování logů (pouze pro logy v takovém systému archivované),
- Manažer KB, Architekt KB a bezpečnostní správci jednotlivých IS (dále jen pracovníci v oblasti bezpečnosti) pouze čtení,
- auditoři (pouze v rámci auditu a se souhlasem Manažera KB) - pouze čtení.

Je-li to technicky možné, mohou mít přístupová práva pro zápis do auditních záznamů pouze pracovníci pověření jejich archivací nebo mazáním starých logů.
Pro zajištění důvěryhodnosti logů musí být dodrženy následující požadavky na oddělení rolí:

- administrátoři provozních zařízení (síťových prvků, serverů, aplikací) nesmí mít přístup k logům uchovávaným v centrálním systému pro sběr logů,
- administrátoři centrálního systému pro sběr logů (případně SIEM) nesmí mít administrátorský přístup k provozním zařízením (mohou však mít přístup pro čtení),
- administrátoři serverů a aplikací nesmějí mít administrátorský přístup k síťovým prvkům a nesmějí mít přístup k IDS,
- administrátoři sítě nesmějí mít, je-li to technicky možné (IDS není součástí síťových prvků) k IDS,
- administrátoři síťových prvků nesmějí mít administrátorský přístup k provozním serverům a aplikacím.

4.10 Logy o činnosti administrátorů a operátorů

Činnosti privilegovaných účtů musí být zaznamenávány do logů. Logy, je-li to technicky a organizačně možné, musejí být chráněny proti narušení ze strany těchto privilegovaných uživatelů. Za nastavení takového logování, je-li technicky možné, odpovídají administrátoři provozních zařízení.

4.11 Synchronizace hodin

Všechny servery, pracovní stanice a další prvky infrastruktury, které používají systémový čas, musí mít pravidelně (minimálně jednou za den) synchronizován systémový čas s centrálním časovým serverem MD nebo jiným zdrojem přesného času, schváleným Odborem ICT.

4.12 Součinnost s provozem centrálního SIEM MD

Provozovatel je povinen na žádost Manažera KB v rozsahu a čase jím stanoveném zajistit předávání logů systému k vyhodnocování do centrálního SIEM MD.

Kapitola 5 ŘÍZENÍ A KONTROLA PROVOZNÍHO SOFTWARU

5.1 Nasazení do provozu

Administrátoři jsou povinni instalovat a udržovat optimalizovanou sadu komponent systému. Optimalizovanou sadou komponent se rozumí pouze komponenty nezbytné pro poskytování služby, pro kterou je prostředek určen, administraci a provozní či bezpečnostní dohled systému. Administrátoři jsou povinni zajistit nespouštění nepotřebných služeb nebo démonů.

Předávání aplikací, systémů, upgrade a nových verzí do provozu se realizuje v souladu s pracovními postupy Odboru ICT. Do provozního prostředí je instalují administrátoři příslušných zařízení, systémů či aplikací.

Pro uvedení nově implementovaných systémů do provozu musí být splněny minimálně tyto podmínky:

- předaná dokumentace včetně bezpečnostní specifikace, havarijních plánů a plánů obnovy je akceptována,
- je akceptován bezpečnostní model (bezpečnostní požadavky specifikované touto přílohou BPI MD, případně další požadavky, uplatněné ze strany MD v rámci daného projektu),
- úspěšné provozní testy,
- úspěšné bezpečnostní testy,
- školení uživatelů i obsluhy (je-li potřebné nebo účelné – rozhodují administrátoři, resp. uživatelé),
- další podmínky specifikované v zadání či řízené dokumentaci.

Splnění výše uvedených podmínek musí potvrdit Architekt KB a schválit Manažer KB.

Je-li nový systém dodáván a implementován externím subjektem, platí po akceptaci stejná pravidla jako pro systémy dodávané a implementované interně.

Smlouva o implementaci musí obsahovat podmínku úspěšného ukončení akceptačních testů před zaplacením implementace (resp. podstatné části této platby).

V případě, že implementace probíhá v samostatných etapách, musí být stanovena akceptační kritéria pro každou etapu.

Administrátoři mohou převzít do provozu pouze zařízení, jehož bezpečnost byla prověřena bezpečnostními testy. Tyto testy musí obsahovat minimálně „scan" na zjištění existence známých zranitelností; případné další testy, které stanoví Manažer KB. Bezpečnostní „scan" provádí Manažer KB nebo jím schválený partner. V případě nasazení mnoha prvků se shodným nastavením, je možné provést testy pouze na vybraném vzorku zařízení.

Je-li to technicky možné, jsou administrátoři povinni nahradit nebo přejmenovat implicitní (defaultní) systémové účty („root", „administrator", „guest", ...).

5.2 Provoz

Administrátoři jsou povinni vytvořit provozní dokumentaci všech spravovaných systémů, která bude obsahovat informace o konfiguraci systému a jejích změnách. Veškeré změny v konfiguraci spravovaných zařízení jsou administrátoři povinni, je-li to účelné, zaznamenávat i do havarijních plánů a plánů obnovy systému po havárii.

Jedno konkrétní zařízení nebo skupinu zařízení ve funkčním celku nesmí spravovat více dodavatelů nebo odborů MD. Počet administrátorů jednotlivých zařízení nebo zařízení ve funkčním celku musí být minimalizován na nejnižší možný počet, který zajistí výkon všech potřebných úkonů a dostatečnou zastupitelnost administrátorů.

Vzdálená správa zařízení, která pracují s informacemi klasifikovanými bezpečnostním klasifikačním stupněm „CHRÁNĚNÉ" a zařízeními umístěnými v DMZ, musí probíhat šifrovaně podle požadavků této přílohy BPI MD (ČÁST VII, Kapitola 1, Odstavec 1.1).

Administrátoři jsou povinni udržovat otevřené pouze porty nezbytné pro zajištění chodu služeb serverů a dalších zařízení ICT. Administrátoři jsou povinni zakázat v systému všechny porty, které nejsou nezbytné pro zajištění chodu služeb serverů, uživatelských stanic a síťových prvků.

Při správě zařízení umístěných v DMZ jsou administrátoři povinni řídit se ustanoveními zvláštního předpisu stanovujícím požadavky na provoz zařízení v DMZ.

Administrátoři jednotlivých zařízení jsou povinni umožnit a zajistit instalaci a konfiguraci bezpečnostního SW definovaného Manažerem KB a potřebné komunikační prostupy. V případě,

že je instalace takového SW nemožná z provozních důvodů, musí tuto skutečnost administrátor prokázat. Za průkazné jsou považovány výstupy z nástrojů pro monitoring systému, známé a zdokumentované potíže s kompatibilitou konkrétních SW komponent a výstupy z provedených testů.

5.3 Pravidelné kontroly

Administrátoři jsou povinni pravidelně (doporučeno je jednou měsíčně) najít soubory, které nemají vlastníka (existuje riziko, že byly do IS MD vloženy neautorizovaně). Administrátor zjistí důvod, proč v systému takové soubory existují, a provede nápravu (smazání, určení vlastníka a podobně).

Administrátoři jsou povinni minimálně jednou měsíčně provést analýzu bezpečnostních logů spravovaných systémů a prověřit případné nalezené anomálie – cílem je zjistit, zda se nejedná o narušení bezpečnosti systému, případně o přípravu k útoku na systém. Odhalení útoku nebo přípravy na něj musí být hlášeno a řešeno jako bezpečnostní incident.

Administrátoři jsou povinni pravidelně (doporučeno je jednou měsíčně) kontrolovat TCP i UDP porty ve stavu „listen". Detekce takového portu, který není uveden v provozní dokumentaci, musí být hlášena a řešena jako bezpečnostní incident. Kontrola TCP i UDP portů se netýká uživatelských stanic.

Administrátoři jsou povinni využívat nástroje pro kontrolu integrity souborového systému.

Manažer KB nebo jím pověřený zaměstnanec je oprávněn provádět v součinnosti s administrátorem namátkové testování zranitelností a slabin. S výsledky těchto testů musí být administrátoři seznámeni a jsou povinni se k nim vyjádřit.

5.4 Instalace softwaru na provozní systémy

Instalaci software na provozní zařízení mohou provádět pouze administrátoři zodpovědní za jeho provoz.

Administrátor odpovídá za to, že na pracovní stanice, servery a další zařízení v jeho správě je instalován pouze software splňující následující podmínky:

- software je potřebný pro výkon činností, správu, dohled, bezpečnost zařízení, bezpečnost IS nebo informačních aktiv MD,
- software je legálně zakoupený, případně se jedná o freeware (i pro komerční použití, např. SW pod GNU licencí a podobně), anebo SW vytvořený interně,
- software je schválen Odborem ICT a není zamítnut Manažerem KB,
- software je schválen administrátorem daného zařízení.

Před instalací software jsou administrátoři povinni ověřit konzistenci a pravost instalačních balíčků (provedení kontroly CRC - Cyclic redundancy check – cyklického redundantního součtu, je-li SW stahován prostřednictvím veřejné datové sítě; provedení kontroly, že se jedná o originální datový nosič od výrobce neumožňující modifikaci dat a podobně).

Pokud nedošlo ke konkrétnímu pověření bezpečnostního správce, administrátoři jsou při správě svěřených zařízení povinni, zajistit, kromě jiného, i bezpečnost zařízení a informací na něm zpracovávaných či uchovávaných.

Kapitola 6 SPRÁVA A ŘÍZENÍ TECHNICKÝCH ZRANITELNOSTÍ

Administrátoři jsou povinni sledovat informace o zranitelnostech a využívat služeb pro sledování zranitelností, které jsou v této oblasti poskytovány. Administrátoři jsou povinni zajistit instalaci relevantních bezpečnostních SW oprav pro daný systém neovlivňujících negativním způsobem běh služeb a aplikací.

Pokud bezpečnostní „patch" negativně ovlivňuje provoz zařízení, musí být jeho (ne)nasazení konzultováno s Manažerem KB tak, aby byla zvážena vhodná kompenzační, případně detekční opatření. Záznam do provozní dokumentace musí být proveden i v případě, že „patch" instalován nebude. Tento záznam musí obsahovat detailní informace o tom, která komponenta zařízení a proč instalaci „patche" neumožňuje, a dále pak patření přijatá pro minimalizaci rizik plynoucích z neinstalování „patche". Pro instalaci bezpečnostních „patchů" musí být minimálně jednou měsíčně vyhrazena časová okna v SLA daného systému.

Nápravná opatření, která jsou administrátorům uložena, mohou být aplikována až na základě souhlasu Manažera KB.

Software na servery a technologická PC mohou instalovat pouze jejich administrátoři a k tomu pověření pracovníci. Na uživatelské stanice mohou instalovat SW i pověření uživatelé, kteří mají přidělena příslušná oprávnění, musí však dodržet ustanovení této přílohy BPI MD.

Kapitola 7 AUDITY IS

Administrátoři jsou povinni poskytnout nezbytné součinnosti pracovníkům provádějícím audit nebo kontrolu podle schváleného plánu auditů a plánu testů (neplánovanou kontrolu musí schválit Manažer KB nebo ředitel Odboru ICT). Bezpečnostní testy jsou prováděny podle pracovního postupu, který definuje Manažer KB.

Pracovníci provádějící audit nebo testy musí mít přístup pouze pro čtení. Je-li pro provedení auditu nebo testů potřebné vyšší přístupové oprávnění, musí být tato skutečnost s administrátory předem konzultována a přístupová oprávnění schválena Manažerem KB. Přístup k auditním záznamům je možný pouze podle pravidel stanovených touto přílohou BPI MD nebo se souhlasem Manažera KB. Konfigurační a systémové soubory mohou být zpřístupněny pouze jako izolované kopie.

Úspěšné provedení penetračních testů (napadení testovaného systému) není považováno za bezpečnostní incident. Penetrační test bez předchozího informování administrátorů, Manažera KB a ředitele Odboru ICT je bezpečnostním incidentem vždy.

ČÁST VII. BEZPEČNOST KOMUNIKACÍ

Obecné bezpečnostní požadavky na správu síťových prvků se řídí příslušnými ustanoveními této přílohy BPI MD.

Kapitola 1 SPRÁVA BEZPEČNOSTI SÍTĚ

Jakékoliv propojení interní sítě s veřejnými datovými sítěmi musí být schváleno administrátory síťové infrastruktury a Manažerem KB. Instalovat komunikační zařízení do sítě MD smějí pouze administrátoři síťové infrastruktury.
Provoz mezi veřejnými sítěmi nebo sítěmi třetích stran a sítí MD musí být řízen pomocí firewallů. Konfigurace FW musí vycházet z principu, co není dovoleno, je zakázáno. Povolené prostupy skrz FW musí být součástí provozní dokumentace; pro každý prostup musí být uveden důvod jeho zřízení.

Služby, poskytované ze sítě MD do prostředí Internetu (webové servery, ftp servery, VPN a podobně) musí být umístěny v DMZ.

Vybrané body propojení sítě MD s veřejnými datovými sítěmi nebo sítěmi třetích stran a rozhraní mezi vybranými bezpečnostními zónami musí být monitorovány a řízeny IDS nebo IPS.

Administrátoři síťové infrastruktury jsou povinni zajistit potřebné propojení pro bezpečnostní monitoring a vyhodnocování dat IDS nebo IPS. Nasazování jednotlivých komponent systému IDS nebo IPS je realizováno dle potřeb MD a schválených zdrojů pro tuto oblast.

Při komunikaci je zakázáno využívat sdíleného média na linkové vrstvě modelu OSI, pokud to nevynucuje technologie.

1.1 Nastavení síťových prvků a jejich vzájemná komunikace

Administrátoři „routerů" i „firewallů" jsou povinni nastavovat základní filtrační pravidla, která vyplývají z RFC (popisujících konkrétní protokoly a podobně).

Pro správu síťových prvků musí být vytvořena fyzicky (nebo na úrovni VLAN) oddělená management síť.

Administrátoři síťových zařízení jsou povinni pro autentizaci vzdálené administrace používat protokolu a serveru „RADIUS", „Diameter", „TACACS+" nebo podobných, případně přistupovat vzdáleně pomocí protokolu „ssh" tam, kde je to možné, nebo využívat jinou bezpečnou technologii schválenou Manažerem KB.

Administrátoři jsou povinni využít prvků autentizace u „routovacích" protokolů a dalšího zabezpečení, které dovoluje implementace těchto protokolů.

1.2 Změny v síťové infrastruktuře

Veškeré změny v síťovém modelu musí být schváleny Manažerem KB. Před realizací takových změn musí být síťovými administrátory sestaven havarijní plán pro případ neúspěšného ukončení nebo musí být nová infrastruktura budována paralelně se stávající.

Změnou v síťovém modelu se rozumí:

- změna oproti pravidlům a požadavkům stanoveným touto přílohou BPI MD, nebo zvláštním předpisem stanovujícím požadavky na provoz v demilitarizovaných zónách,
- modifikace propojení nebo struktury jednotlivých síťových segmentů či vytvoření nových,
- změna v IP plánu,
- změny statických „routovacích" pravidel a „routovacích" tabulek,
- změny, které by mohly mít dopady na funkčnost bezpečnostních prvků, např.:
  - změny ve struktuře evidencí síťových prvků a prostupů mezi síťovými segmenty či sítěmi,
  - změny v konfiguraci IDS zařízení v síťových prvcích,
  - libovolné změny v konfiguraci segmentů sítě, které slouží pro přenos dat mezi bezpečnostními systémy.
- zavádění nových technologií,
- a další, které administrátoři síťové infrastruktury budou považovat za zásadní.

1.3 Bezpečnost bezdrátových sítí

Instalaci zařízení pro poskytování služeb bezdrátové sítě mohou provádět pouze k tomu pověření pracovníci provozních útvarů se souhlasem administrátorů síťové infrastruktury.

Administrátoři jsou povinni nastavit zařízení umožňujících bezdrátový přístup do sítě MD tak, aby byly naplněny minimálně tyto požadavky:

- zařízení nesmí umožňovat anonymní přístup,
- pro autentizaci zařízení k bezdrátové síti musí být použit minimálně jeden z těchto mechanismů:
  - uživatelský certifikát vydaný interní CA – Certifikační autorita MD – nebo jinou důvěryhodnou certifikační autoritou schválenou manažerem KB,

- 802.1x mechanismus s centrálním autentizačním prvkem,
- pro ochranu komunikace musí být použito minimálně WPA2,
- musejí být vytvářeny auditní záznamy o připojených zařízeních obsahující minimálně datum a čas připojení nebo odpojení zařízení, jeho MAC adresu a IP adresu.

Zařízení, která nesplňují výše uvedené požadavky, nesmějí být do interní sítě MD připojena. Provoz takových zařízení je možný pouze v případě, že umožňují přístup (jsou propojena) pouze přímo do Internetu.

Manažer KB nebo jím pověřený zaměstnanec je oprávněn provádět detekci a testy bezdrátových sítí v okolí provozních prostor MD.

1.4 Internetová gateway pro uživatele

Uživatelé (zaměstnanci MD i externisté) mohou přistupovat k Internetu pouze přes centrální přístupovou" gateway" nebo "proxy" server. Administrátoři této „gateway" jsou povinni:

- nastavit prostupy pouze pro povolené protokoly na povolených portech,
- umožnit komunikaci s a přes tuto „gateway" pouze z interní sítě MD.

Povolené protokoly a porty pro komunikaci uživatelů do Internetu jsou:

- http (80),
- https (443),
- ftp (20, 21),
- další pouze na základě výjimky, schválené Manažerem KB.

Administrátoři této „gateway" jsou povinni na ni zajistit logování přístupu uživatelů k Internetu a jeho využívání. Události musí být logovány minimálně v rozsahu:

- zdrojová IP adresa,
- přihlašovací jméno (např. z Active Directory MD) nebo jiné jednoznačné určení uživatele,
- datum a čas,
- požadované „url".

Tyto logy musí být ve všech kopiích klasifikovány přinejmenším bezpečnostním klasifikačním stupněm „PRO VNITŘNÍ POTŘEBU". Administrátoři jsou povinni tyto logy uchovávat minimálně po dobu jednoho roku a na vyžádání je poskytnout Manažerovi KB.

Kapitola 2 VZDÁLENÉ PŘÍSTUPY DO IS MD

Veškeré klientské přístupy musí být konfigurovány tak, aby neumožnily připojení zařízením, která nesplní definovanou bezpečnostní politiku pro přístup. Tato politika musí obsahovat minimálně:

- definici autentizačních mechanismů (silná autentizace, vícefaktorová autentizace),
- definici šifrovacích algoritmů,
- definici technologií pro VPN spojení,
- zákaz jakýchkoliv dalších síťových připojení na klientském zařízení.

Administrátoři klientských zařízení používaných pro vzdálený přístup k síti MD je musí konfigurovat tak, aby vyhověly výše uvedené politice.

Pro „site-to-site" přístupy musí být definována bezpečnostní politika, která musí obsahovat minimálně:

- definici autentizačních mechanismů – důvěryhodný certifikát nebo bezpečně vyměněný „pre-shared" klíč (délka alespoň 20 znaků, použití velkých a malých písmen, číslic a speciálních znaků),
- definici šifrovacích algoritmů,

- definici technologií pro VPN spojení.

Za definici těchto politik zodpovídají administrátoři serverových zařízení pro vzdálený přístup. Všechny tyto politiky (a jejich změny či aktualizace) musí být před aplikací schváleny Manažerem KB.

Vzdálené přístupy externích subjektů musí být schváleny Manažerem KB.

2.1 Práce na dálku

K síti MD mohou vzdáleně přistupovat zaměstnanci, dodavatelé, externí spolupracovníci a další. Pro tyto přístupy musí být vytvořeny oddělené přístupové body:

- klientský přístup pro zaměstnance MD,
- klientský přístup pro externisty,
- přístup pro dodavatele, kteří na MD pracují na implementaci systémů („site-to-site"),
- přístup pro dodavatele, kteří na MD provádějí externí správu zařízení („site-to-site").

Veškeré „site-to-site" VPN mohou dodavatelům zpřístupňovat pouze nezbytně nutnou část infrastruktury.

ČÁST VIII. AKVIZICE, VÝVOJ A ÚDRŽBA SYSTÉMŮ

Kapitola 1 BEZPEČNOSTNÍ POŽADAVKY

Bezpečnostní požadavky systémů musí splňovat veškeré zákonné požadavky na informace v těchto systémech zpracovávané a dále musí splňovat požadavky stanovené touto přílohou BPI MD.

Aplikace nesmí pracovat s informacemi, které nejsou pro její fungování potřebné. Po síti (interní i veřejné) mohou být přenášena pouze data, ke kterým má uživatel či aplikace na základě svých oprávnění přístup; jiné informace nesmějí být přenášeny ani skrytě.

1.1 Analýza a specifikace požadavků

Základní bezpečnostní požadavky musejí být součástí prvotní analýzy připravovaného software i jeho jednotlivých komponent. V závislosti na plánovaném použití software a jeho architektuře mohou být Manažerem KB stanoveny další požadavky vyplývající z analýzy rizik.

Při formulaci požadavků a výběru řešení musí být zohledněny zejména tyto skutečnosti:

- naplnění zákonných požadavků a požadavků, uvedených v BPI MD a v jejích přílohách,
- kapacity provozních útvarů a útvarů provádějících akceptační (provozní i bezpečnostní) testy,
- dřívější bezpečnostní a provozní incidenty,
- další požadavky Manažera KB a výsledky analýzy rizik,
- naplnění dalších předem stanovených výběrových (provozních, bezpečnostních, uživatelských a podobně) kritérií.

1.2 Zabezpečení aplikačních služeb ve veřejných sítích

Aplikační služby provozované ve veřejných datových sítích musí dále splňovat:

- všechny servery musí pro ověření (své) identity a šifrování při komunikaci s klienty používat certifikáty schválené MD,
- komunikace se servery partnerů musí být zajištěna šifrováním a autentizace serverů certifikáty,

- veškerá komunikace (včetně autentizace uživatelů) musí být šifrována dle požadavků této přílohy BPI MD (tj. aplikace nedělají ani „redirect" z HTTP na HTTPS, spojení může být navázáno pouze na HTTPS),
- na front-end serverech nesmí být trvale uchovávána data a nesmí obsahovat databáze uživatelů,
- veškeré přístupy uživatelů musí být logovány podle požadavků této přílohy BPI MD,
- servery musí být od veřejných sítí odděleny FW, může být povolena pouze definovaná komunikace,
- serverům provozujícím různé služby zákazníkům nesmí být kromě nezbytné aplikační výměny dat umožněna vzájemná komunikace.

1.3 Ochrana transakcí aplikačních služeb

Ochrana transakcí aplikačních služeb musí splňovat minimálně tyto požadavky:

- aplikace nebo systém musí splnit všechny požadavky stanovené touto přílohou BPI MD,
- pro veškeré transakce musí být použito potvrzení elektronickým podpisem (na straně koncových uživatelů může být nahrazen OTP nebo druhým autentizačním faktorem),
- veškerá komunikace mezi všemi komponentami systému musí být šifrována pomocí certifikátů (komunikace s koncovým uživatelem může být šifrována ad hoc),
- musí být definován seznam schválených důvěryhodných certifikačních autorit, certifikáty jiných CA nesmějí být akceptovány,
- administrátoři aplikace nebo systému jsou povinni zkontrolovat dodržování certifikační politiky (minimálně obnova „root" certifikátu, pravidelnost vydávání CRL, povolený způsob využití certifikátů) každé schválené CA před provedením konfigurace, která umožní akceptaci certifikátů vydaných danou autoritou; tuto kontrolu musí administrátoři opakovat minimálně jednou za šest měsíců a o jejím provedení musí učinit záznam do provozní dokumentace,
- certifikáty protistrany musí být ověřeny (podpis certifikátem vydávající CA, kontrola CRL),
- konfigurace kryptografických prostředků aplikací je možná bez zásahu do aplikace pouhou změnou konfigurace, tj. není nutné programování,
- na „frontendových" serverech nesmějí být trvale uchovávány žádné uživatelské ani transakční údaje,
- přístup k datům smí být umožněn pouze přes aplikaci na frontendovém serveru,
- transakční data musí být uložena šifrovaně, administrátorům nesmí být k těmto údajům umožněn přístup,
- veškeré použité šifrovací algoritmy a délky klíčů musí splňovat požadavky této přílohy BPI MD.

Kapitola 2 BEZPEČNOST V PROCESECH VÝVOJE A PODPORY

Při vývoji SW musí být dodrženy minimálně tyto podmínky:

- vyvíjené aplikace a systémy musí umožnit naplnění všech ustanovení této přílohy BPI MD (zejména řízení přístupu, politika hesel, logování, ochrana komunikace, zálohování),
- bezpečnostní model a další bezpečnostní požadavky musí být definovány před zahájením prací na vývoji aplikace nebo systému,
- při vývoji aplikace nebo systému musí být dodrženy metodiky pro bezpečný vývoj a provoz a správu IS nebo jejich relevantní části (např. ITIL – Information Security Infrastructure Library, OWASP – Open Web Application Security Project, PCI DSS – The Payment Card Industry Data Security Standard,...) a doporučení výrobců vývojových nástrojů, existují-li,

- vývojové prostředí musí být odděleno od provozního i testovacího, přístup do vývojového prostředí mohou mít pouze pověření pracovníci,
- pro vývoj podobě jako pro testování nesmějí být použita ostrá data,
- zdrojové kódy aplikací ve správě nebo vlastnictví MD musí být klasifikovány přinejmenším klasifikačním stupněm „PRO VNITŘNÍ POTŘEBU“ (a podle této klasifikace s nimi musí být nakládáno),
- u aplikací a systémů dodávaných na klíč musí být smluvně zajištěno, že zdrojové kódy budou majetkem MD,
- aplikace musí pracovat pod vlastním účtem, který nemá superuživatelská oprávnění,
- musí být uplatněna zásada minimální manipulace s daty (aplikace nebo její funkční části nepracují s daty a nepřistupují k datům, která nejsou pro vykonávanou činnost potřeba) a minimálních přístupových práv (aplikace nebo její funkční části mají pouze taková oprávnění, která potřebují pro vykonávanou činnost),

Je-li vývoj realizován externě, musí dodavatel předem potvrdit dodržení ustanovení této kapitoly.

Kapitola 3 DATA PRO TESTOVÁNÍ

Testování nesmí probíhat nad ostrými daty. Pro potřeby testování musí být vytvořena vlastní data, která obsahem neodpovídají produkčním datům (při zajištění dostatečné vypovídající hodnoty testování).

ČÁST IX. ŘÍZENÍ INCIDENTŮ BEZPEČNOSTI INFORMACÍ

Kapitola 1 ODPOVĚDNOST A POSTUPY

Povinnosti uživatelů i administrátorů a příslušné postupy pro zvládání bezpečnostních incidentů jsou podrobně popsány v Příloze č. 11.

Vlastníci informačních aktiv a správci IS jsou povinni činit taková opatření, aby nedocházelo ke vzniku bezpečnostních incidentů.

Administrátoři jsou zejména povinni dbát na předcházení bezpečnostním incidentům (jsou povinni zajistit zejména nepřetržité automatizované vyhodnocování bezpečnostních událostí) a neprodleně reagovat v případě, že bezpečnostní incident nastane.

Bezpečnostními incidenty se rozumí stav systému, služby nebo sítě, ukazující na možné porušení bezpečnosti informací (obecně nebo vyplývající z bezpečnostní dokumentace) nebo selhání bezpečnostních opatření.

Kapitola 2 PODÁVÁNÍ ZPRÁV O INCIDENTECH BEZPEČNOSTI INFORMACÍ

Hlášení bezpečnostních incidentů se provádí dle ustanovení v Příloze č. 11.
Administrátoři systémů, kterých se nalezený bezpečnostní incident dotýká, jsou dále povinni:

- bezodkladně zasáhnout přiměřeným způsobem tak, aby znemožnili pokračování zjištěného nežádoucího stavu,
- bezodkladně informovat MD způsobem dohodnutým se správcem IS a s Manažerem KB,
- zajistit veškeré dostupné auditní záznamy pro případ jejich potřeby při vyšetřování bezpečnostního incidentu či přípravě a realizaci nápravných opatření. Tyto záznamy jsou administrátoři na vyžádání povinni předat pracovníkům v oblasti bezpečnosti,
- řešit (případně navrhnout řešení) následky bezpečnostního incidentu,

- provést kontrolu všech systémů, které by mohly být incidentem zasaženy, resp. informovat administrátory těchto systémů,
- najít a odstranit příčiny vzniku bezpečnostního incidentu, resp. požadovat nápravu u příslušných útvarů MD nebo dodavatelů. Není-li náprava možná je administrátor povinen informovat Manažera KB a svého nadřízeného a spolupracovat při návrhu a implementaci alternativního řešení.

Kapitola 3 PODÁVÁNÍ ZPRÁV O ZRANITELNOSTECH BEZPEČNOSTI INFORMACÍ

Zranitelnost je nedostatek, který umožňuje uplatnění hrozby, resp. překonat stávající bezpečnostní opatření, např. využívat IS MD v rozporu s přidělenými přístupovými právy.

Všichni zaměstnanci jsou povinni informovat o zjištění zranitelnosti a nahlásit ji v rámci Incident Managementu jako možné riziko.

Administrátoři systémů, kterých se nalezená zranitelnost dotýká, jsou dále povinni:

- informovat o zranitelnosti administrátory dalších systémů, které mohou být podobně postiženy, nadřízeného zaměstnance a Manažera KB,
- zdokumentovat nalezenou zranitelnost a navrhnout řešení na její eliminaci. Navržené řešení musí být před implementací schváleno Manažera KB,
- provést potřebné zásahy na dotčeném systému,
- v případě, že slabina byla nalezena na systému podporovaném, resp. spravovaném jeho výrobcem či dodavatelem (interním i externím), informovat jej o bezpečnostní zranitelnosti a požadovat nápravu. Není-li náprava možná je administrátor povinen informovat Manažera KB a svého nadřízeného a spolupracovat při návrhu a implementaci alternativního řešení resp. kompenzačního opatření.

K posouzení a rozhodnutí o událostech bezpečnosti informací je oprávněn Manažer KB.

Kapitola 4 ODEZVA NA INCIDENTY BEZPEČNOSTI INFORMACÍ

Při stanovení bezpečnostních požadavků jsou odpovědné osoby povinny zohledňovat skutečnosti, které byly v minulosti rozhodné pro vznik bezpečnostního incidentu.

Způsob řešení bezpečnostního incidentu je administrátor povinen zaznamenat do systémové dokumentace a případně i do havarijních plánů (doporučeno odkazem na dokumentaci). Záznam musí obsahovat identifikaci "kořenové příčiny" incidentu, tedy bod, kde incident opravdu vznikl, nikoliv pouze bod, kde se incident projevil.

Znalosti získané z analýz a řešení bezpečnostních incidentů jsou povinni zaměstnanci zohlednit v návrzích při zavádění produktů a služeb v rámci MD tak aby se snížila pravděpodobnost nebo dopady následných incidentů.

Kapitola 5 SHROMAŽĎOVÁNÍ DŮKAZŮ

V rámci šetření bezpečnostních incidentů jsou administrátoři povinni:

- předat nebo zpřístupnit pracovníkům v oblasti bezpečnosti, pověřeným šetřením incidentů veškeré vyžádané dostupné logy ze systémů ve své správě (záznamy podléhající zvláštnímu režimu mohou administrátoři předat pouze v souladu s pravidly, danými platnými právními předpisy),
- předat nebo zpřístupnit pracovníkům v oblasti bezpečnosti pověřeným šetřením incidentů veškerou vyžádanou provozní dokumentaci systémů ve své správě,

- nastavit na vyžádání detailnější logování dle požadavků pracovníků v oblasti bezpečnosti pověřených šetřením incidentů, pokud to negativně neovlivní provoz systému,
- předat pracovníkům v oblasti bezpečnosti pověřeným šetřením incidentů veškeré další požadované dostupné informace o konfiguraci a provozu systémů ve své správě.

ČÁST X. ŘÍZENÍ KONTINUITY ČINNOSTÍ

Podrobněji jsou požadavky na havarijní plány popsány v příloze č. 9, na řízení incidentů a problémů pak v přílohách č. 10 a 11.

ČÁST XI. SOULAD S POŽADAVKY

Administrátoři systémů a zařízení jsou povinni dodržovat obecně závazné právní předpisy.

Administrátoři MD jsou povinni dodržovat pravidla a bezpečnostní opatření definovaná interní bezpečnostní dokumentací MD.

ČÁST XII. PŘECHODNÁ USTANOVENÍ

Do doby zajištění technických prostředků a podmínek pro dodržování pravidel pro provozovatele je nutné postupovat v co největší možné míře souladu s touto přílohou BPI MD.