



Česká republika – Ministerstvo vnitra

se sídlem: Nad Štolou 936/3, 170 34 Praha 7

IČ, DIČ: 00007064, CZ00007064

Za níž jedná: Mgr. Bohdan Urban, ředitel odboru eGovernmentu na základě usnesení řídicího výboru projektu ze dne 22. 12. 2014

Kontaktní adresa: Náměstí Hrdinů 1634/3, 140 21 Praha 4

dále jen „**Objednatel**“ na straně jedné

č. smlouvy Objednatele: MV-161698- 16/EG-2014

a

Česká pošta, s.p., Odštěpný závod ICT služby

se sídlem: Olšanská 1951/4, 130 00 Praha 3

IČ, DIČ: 47114983, CZ47114983

bankovní spojení: ČSOB a.s., č. ú.: 117404973/0300

zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl A, vložka 7565

Za níž jedná: Jan Přerovský, vedoucí Odštěpného závodu ICT služby

dále jen „**Dodavatel**“ na straně druhé

č. smlouvy Dodavatele: 2014/089 OZ ICT

(dále také společně označováni jako „**Smluvní strany**“)



Článek 1. Úvodní ustanovení

Vzhledem k tomu, že:

- 1.1 Vláda České republiky schválila svým usnesením č. 224, ze dne 4. dubna 2012, Informaci o zajištění vybraných služeb informačních a komunikačních technologií využívaných státní správou a změnu Zakládací listiny státního podniku Česká pošta, s. p., spočívající v rozšíření předmětu činnosti České pošty, s.p., o výkon vybraných služeb;
- 1.2 z postavení Dodavatele, vůči němuž Objednatel vykonává funkci zakladatele podle zákona č. 77/1997 Sb., o státním podniku, ve znění pozdějších předpisů, a charakteru Díla (jak je tento pojem dále definován) vyplývá možnost, aby Objednatel zadal realizaci Díla Dodavateli, neboť podmínky podle § 18 odst. 1 písm. e) zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů, pro zadání veřejné zakázky mimo režim zákona, jsou v daném případě splněny;
- 1.3 Právní vztah založený touto Smlouvou se bude řídit ustanovením § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**Občanský zákoník**“) a zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „**Autorský zákon**“), jakož i některými dalšími zvláštními právními předpisy upravujícími závazné podmínky ve vztahu k předmětu plnění této Smlouvy;
- 1.4 Projektový záměr, jenž je Přílohou č. 1 Smlouvy, byl vytvořen pro podporu investice do Dohledového centra MV pro provoz ICT systémů a kybernetickou bezpečnost (SOCCR) (dále jen „**Dohledové centrum SOCCR**“). Dohledové centrum SOCCR rozšiřuje funkčnost servisní platformy eGovernmentu v rámci Centrálního místa služeb a naplňuje požadavky zákona č. 181/2014 Sb. o kybernetické bezpečnosti. Dohledové centrum SOCCR je navrženo plně v souladu se schválenou Strategií kybernetické bezpečnosti na roky 2012 – 2015, stejně tak s budoucí, zatím neschválenou, strategií na roky 2015 – 2020 (ve fázi přípravy).
- 1.5 Dodavatel prohlašuje, že jsou mu známy veškeré dokumenty, podmínky a materiály týkající se projektů ITS NGN, KSP, NIS IZS a CMS, a to včetně všech případných změn u těchto projektů, a že budou zohledněny v maximální možné míře pro tvorbu Dohledového centra SOCCR a zejména architektury Dohledového centra SOCCR. Dále Dodavatel prohlašuje, že mu nejsou známy žádné omezující podmínky zejména z projektů kofinancovaných v rámci IOP navazujících na Dohledové centrum SOCCR;
- 1.6 Na základě projednání Komise pro kybernetickou bezpečnost bylo dne 10. 12. 2014 rozhodnuto, že Dodavatel bude následně rovněž provozovatelem Dohledového centra SOCCR;
- 1.7 Dodavatel prohlašuje, že disponuje všemi příslušnými oprávněními k podnikání nezbytnými pro řádné plnění předmětu této Smlouvy a dále prohlašuje, že disponuje veškerými technickými, ekonomickými i personálními předpoklady pro řádné plnění předmětu této Smlouvy, a to zejména:
 - 1.7.1 prostřednictvím moderních logistických služeb má schopnost zajistit služby s přidanou hodnotou, které dále zefektivní zajišťované služby;



1.7.2 má silnou kompetenci v oblasti centralizovaných nákupních procesů a má schopnost zajistit administraci celého zadávacího procesu, od analýzy poptávaných komodit, administraci předmětného zadávacího řízení, po zajištění distribuce.

1.5. Na základě projednání Komise pro kybernetickou bezpečnost uzavírají níže uvedeného dne, měsíce a roku tuto

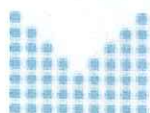
Smlouvu o dílo na vytvoření Dohledového centra MV pro provoz ICT systémů a kybernetickou bezpečnost (SOCCR)
(dále jen „Smlouva“)

Článek 2.

Definice některých pojmů a zkratk

2.1. Při výkladu obsahu Smlouvy budou níže uvedené pojmy a zkratky vykládány takto:

Dodavatel, ČPOZ	Česká pošta s.p., Odštěpný závod ICT služby
CMS	Centrální místo služeb
ITS	Integrovaná telekomunikační síť Ministerstva vnitra ČR
ITS NGN	Zajištění infrastruktury pro operační střediska základních složek IZS, Integrovaná telekomunikační síť MV
NIS IZS	Národní informační systém integrovaného záchranného systému
KSP	Krajské standardizované projekty HZS krajů a Centrální standardizovaný projekt generálního ředitelství HZS ČR
AIS	Agendový informační systém
BCM (Business Continuity Management)	Oblast řízení, která je zaměřena na to, aby byly trvale dostupné všechny kritické funkce organizace vůči zákazníkům, dodavatelům a dalším stranám
ČR	Česká republika
DC	Dohledové centrum
DR (Disaster Recovery)	Předem připravený scénář, který vede k obnově infrastruktury po nastalé havárii
FTE (Full Time-Equivalent)	Ukazatel, jenž vypovídá o stupni zapojení zaměstnance na projektu.
MV ČR, Objednatel	Ministerstvo vnitra České republiky
eGov	Odbor eGovernmentu Ministerstva vnitra ČR
OSF	Odbor strukturálních fondů Ministerstva vnitra České republiky



ZDTP	Změny detailů technického projektu
Systémový integrátor	Systémová integrace znamená spojení různých komponent ICT technologií nebo subsystémů v jeden fungující celek. Dodavatelem služby systémové integrace je systémový integrátor.
KIVS	Komunikační infrastruktura veřejné správy, jak je specifikována Usnesením vlády ČR č. 385 ze dne 30. 5. 2012 v souladu s Dohodou o centralizovaném zadávání, uvedenou v bodu 2 písm. a) tohoto usnesení.
HoneyPot	Informační systém, který emuluje chod standardních systémů nebo sítí. Slouží k včasnému odhalení neoprávněné komunikace.
HW	Hardware
IPS/IDS (Intrusion Prevention / Deception System)	Systém pro prevenci nebo detekci průniku do sítě
ISMS (Information Security Management System)	Systém řízení a správy informačních aktiv
IOP	Integrovaný operační program
NBA-Netflow (Network Behavioral Analysis)	Analytický nástroj pro zjištění chování sítě
NBU	Národní bezpečnostní úřad
NCKB	Národní centrum kybernetické bezpečnosti
OS	Operační systém
OVM	Orgán veřejné moci
Projekt	Dohledové centrum MV pro provoz ICT systémů a kybernetickou bezpečnost (SOCCR)
SIEM (Security Incident & Event Management)	Systém pro správu událostí a řízení bezpečnosti
SOCCR (Security Operation Center for Continuous Reliability)	Dohledové centrum SOCCR
SW	Software
ZoKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů

2.2. Definice některých dalších pojmů a zkratk jsou obsaženy dále v textu Smlouvy a jejích přílohách.



Článek 3. Předmět Smlouvy

- 3.1. Předmětem této Smlouvy je vytvoření Dohledového centra SOCCR, jehož projektový a investiční záměr v aktuální podobě je uveden v Příloze č. 1 této Smlouvy (dále jen „Dílo“ nebo „Předmět plnění“).
- 3.2. Dodavatel se zavazuje k provedení Díla na svůj náklad a nebezpečí a Objednatel se zavazuje řádně provedené Dílo převzít a zaplatit cenu za jeho provedení za podmínek a ve výši sjednané touto Smlouvou.
- 3.3. Předmět plnění je rozdělen na 5 částí uvedených v Příloze č. 3 Smlouvy, přičemž Část 1 Předmětu plnění je vypracování Technického projektu, který bude zahrnovat detailní investiční záměr a detailní popis architektury, procesů a funkcionalit Dohledového centra SOCCR. Požadavky na vypracování Technického projektu jsou uvedeny v Příloze č. 2 Smlouvy. Každá Část Předmětu plnění je dílčím plněním Předmětu plnění a fakturačním milníkem.
- 3.4. Po řádném předání a převzetí (akceptaci) Části 1 Předmětu plnění bude podrobně vyspecifikováno plnění zbývajících částí Předmětu plnění.

Článek 4. Místo a doba plnění

- 4.1. S ohledem na charakter plnění této Smlouvy je místem jejího plnění celá Česká republika, zejména pak sídlo Objednatele. Umožňuje-li to povaha plnění, je Dodavatel oprávněn provádět Dílo také prostřednictvím vzdáleného přístupu.
- 4.2. Veškeré písemné výstupy ze své činnosti bude Dodavatel předávat na kontaktní adrese Objednatele, nebude-li v konkrétním případě sjednáno jinak.
- 4.3. Dodavatel je povinen provést Předmět plnění v souladu s harmonogramem plnění, který tvoří Přílohu č. 3 Smlouvy.
- 4.4. Harmonogram plnění bude v případě potřeby upraven po řádném předání a převzetí Části 1 Předmětu plnění, a to ve formě dodatku ke Smlouvě uzavřeného v souladu s čl. 20.6 Smlouvy.
- 4.5. Dodavatel se zavazuje, že Dílo předá nejpozději ke dni 30. 11. 2015.

Článek 5. Cena Díla

- 5.1. Smluvní strany se dohodly, že celková cena za Dílo nepřesáhne 56.113.000,- Kč (slovy: padesát šest milionů jedno sto třináct tisíc korun českých), včetně zákonné sazby DPH ke dni podpisu Smlouvy. Tato celková cena je stanovena jako cena maximální, nejvýše přípustná, nepřekročitelná a zahrnující veškeré náklady Dodavatele spojené s plněním Předmětu plnění dle této Smlouvy.
- 5.2. Celková cena za Část 1 Předmětu plnění – Technický projekt dle čl. 3 odst. 3.3 této Smlouvy činí 4.808.000,- Kč (slovy: čtyři miliony osm set osm tisíc korun českých),



včetně zákonné sazby DPH ke dni podpisu Smlouvy (slovy: pět milionů osm set sedmnáct tisíc šest set osmdesát korun českých). Tato cena je nepřekročitelná.

- 5.3. Cena za ostatní Části Předmětu plnění, které budou specifikovány po řádném předání a převzetí (akceptaci) Části 1 Předmětu plnění, činí nejvýše částku uvedenou v tabulce v odst. 5.6 této Smlouvy. Tyto ceny budou upřesněny po řádném předání a převzetí Předmětu plnění dle čl. 3 odst. 3.3 (Část 1), a to po upřesnění položkového rozpisu a záručních podmínek těchto Částí v souladu s Technickým projektem, a to formou dodatku ke Smlouvě. Pro vyloučení všech pochybností se stanovuje, že součet celkové ceny za ostatní Části Předmětu plnění, uvedený v tabulce níže, tj. 51.305.000,- včetně zákonné sazby DPH ke dni podpisu Smlouvy, je nepřekročitelný.
- 5.4. Cena za části plnění případně poskytované subdodavateli bude Objednateli účtována ve výši skládající se z ceny, v jaké ji Dodavatel od subdodavatelů pořídí a obchodní marže Dodavatele ve výši 10 %. Uvedená marže Dodavatele je již zahrnuta v rámcovém rozpočtu, který je součástí přílohy č. 1 této Smlouvy. Upřesnění části ceny Předmětu plnění dle čl. 5 odst. 5.3 Smlouvy na základě všech subdodavately provedených částí plnění bude provedeno vždy ve formě dodatků ke Smlouvě, které budou obsahovat položkový rozpočet odsouhlasený Smluvními stranami, přičemž horní limit celkové ceny za dílo uvedený v čl. 5 odst. 5.1 Smlouvy je nepřekročitelný. Smluvní strany uzavrou po skončení dílčích výběrových řízení (veřejných zakázek) realizovaných Dodavatelem na dílčí části Předmětu plnění Dodatky, kterými bude jednoznačně specifikováno dílčí plnění včetně individuálních cen jednotlivých položek Předmětu plnění, a to v souladu s vymezením příslušné části plnění poskytované daným subdodavatelem a v souladu s cenou této části plnění sjednané s daným subdodavatelem.
- 5.5. Výše cen uvedených v čl. 5 odst. 5.3 Smlouvy bude upřesněna dle výsledků výběrových řízení v souladu s odst. 5.4 Smlouvy a dále dle skutečně odpracovaných člověkodnů („MD“) v rámci služeb poskytovaných Dodavatelem. Smluvně stanovené ceny MD pro jednotlivé role členů řešitelského týmu Dodavatele v rámci realizace Díla jsou uvedeny v Příloze č. 4 Smlouvy a zahrnují marži Dodavatele ve výši uvedené v čl. 5 odst. 5.4 Smlouvy. Počet odpracovaných MD je Dodavatel povinen vykazovat měsíčně v rámci Zprávy o stavu Projektu, která je definována v Příloze č. 5 Smlouvy. Výkaz odpracovaných MD za dílčí plnění bude také předkládán Objednateli ke schválení nejpozději 5 pracovních dní přede dnem vystavení faktury dle čl. 6 Smlouvy. Výkaz odpracovaných MD musí obsahovat:
- 5.5.1. údaj o období, za které je výkaz zpracován,
 - 5.5.2. jmenný seznam členů řešitelského týmu s uvedením rolí jednotlivých členů,
 - 5.5.3. údaje o výši pracovního úvazku jednotlivých členů řešitelského týmu během období, za které je výkaz odpracovaných MD zpracován,
 - 5.5.4. údaje o počtu MD, jež jednotliví členové řešitelského týmu odpracovali při realizaci Předmětu plnění v období, za něž je výkaz odpracovaných MD zpracován.
- 5.6. Smluvní strany uvádí ceny za jednotlivé Části Předmětu plnění v této tabulce:



Část plnění	Dílčí plnění	Cena bez DPH	DPH ve výši 21%	Cena včetně DPH
Část 1	Technický projekt			
	Celkem za Část 1	3.973.553,72 Kč	834.446,28 Kč	4.808.000,- Kč
Ostatní Části				
	Celkem za ostatní Části (tj. za 4 zbývajících dílčí plnění)	42.400.826,44 Kč	8.904.173,56 Kč	51.305.000,- Kč
Celkem		46.374.380,16 Kč	9.738.619,84 Kč	56.113.000,- Kč

- 5.7. Ceny uvedené v tomto článku jsou uvedeny jako ceny bez DPH a s DPH ve výši platné ke dni uzavření Smlouvy. Dojde-li ke změně sazby DPH, bude DPH účtována podle právních předpisů platných v době uskutečnění zdanitelného plnění. Takováto změna ceny není důvodem k uzavření dodatku ke Smlouvě.

Článek 6.

Platební podmínky

- 6.1. Právo na zaplacení ceny dílčího plnění vzniká Dodavateli řádným a včasným předáním a převzetím dílčího plnění na základě písemné akceptace Objednatele, a to nejdříve po sjednaném termínu dílčího plnění v souladu s harmonogramem v Příloze č. 3 Smlouvy na základě daňového dokladu (faktury) vystavené Dodavatelem. Datum uskutečnění zdanitelného plnění (dále jen „DUZP“) bude stanoveno datem schváleného Akceptačního protokolu. Přílohou takto vystavené faktury bude kopie Akceptačního protokolu, potvrzeného Smluvními stranami a výkaz odpracovaných MD dle čl. 5 odst. 5 Smlouvy, potvrzený Smluvními stranami.
- 6.2. Při realizaci Díla nejsou přípustné vícenáklady. Objednatel nebude poskytovat zálohové platby.
- 6.3. Faktury musí mít obecné náležitosti daňových dokladů podle ustanovení § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, náležitosti obchodních listin dle ustanovení § 435 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů a musí v nich být uvedeno číslo Smlouvy Objednatele. Faktury budou doloženy předávacím protokolem potvrzeným oprávněným zástupcem Objednatele, který bude nedílnou součástí faktury.
- 6.4. Přílohou faktury musí být položkový rozpis fakturovaného plnění (vč. výkazu odpracovaných MD), který bude zpracován v rozsahu a v podrobnostech nezbytných pro řádný výkon kontroly Objednatele dle ustanovení § 14 odst. 2 vyhlášky č. 416/2004 Sb., kterou se provádí zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole).
- 6.5. Faktury budou zasílány na kontaktní adresu Objednatele, uvedenou v záhlaví této Smlouvy.



- 6.6. Faktura je splatná do 30 kalendářních dnů ode dne jejího prokazatelného doručení Objednateli. Za den úhrady faktury se považuje den odepsání příslušné částky z účtu Objednatele a její zaslání ve prospěch účtu Dodavatele.
- 6.7. Pokud bude faktura doručena v období mezi 16. prosincem a 28. únorem příslušného kalendářního roku Smluvní strany se dohodly, že na žádost Objednatele Dodavatel prodlouží splatnost faktury na 60 kalendářních dnů ode dne doručení.
- 6.8. Dodavatel se zavazuje, že poslední zdanitelné plnění v rámci Díla bude uskutečněno nejpozději ke dni 15.12.2015.
- 6.9. Objednatel si vyhrazuje právo vrátit bez zaplacení fakturu, která není vystavena v souladu s touto Smlouvou, a to do 10 kalendářních dnů ode dne obdržení faktury. Oprávněným vrácením faktury přestane běžet původní doba splatnosti. Po opravě faktury Dodavatelem běží nová lhůta splatnosti 30 kalendářních dnů, resp. 60 dnů v případě faktur dle čl. 6.7 Smlouvy, ode dne doručení opravené nebo nově vyhotovené faktury.
- 6.10. Veškeré platby podle Smlouvy budou probíhat výlučně bezhotovostním převodem v české měně. V případě, že v České republice dojde k zavedení EUR jakožto úřední měny České republiky, bude proveden přepočítání ceny na EUR, a to podle úředně stanoveného směnného kursu. Veškeré platby za plnění Smlouvy budou ode dne zavedení EUR, jakožto úřední měny České republiky, hrazeny pouze v EUR.
- 6.11. Dodavatel se zavazuje, že nedojde k duplicitnímu plnění dle této Smlouvy a jiných smluvních vztahů uzavřených s Českou republikou – Ministerstvem vnitra. Na základě žádosti Objednatele je Dodavatel v souladu s čl. 6.4 Smlouvy povinen poskytnout nezbytnou součinnost Objednateli k ověření, že nedochází k duplicitnímu financování činností Dodavatele. Za tím účelem je Dodavatel především povinen předložit doklady vyžádané Objednatelem.

Článek 7.

Předání, převzetí a akceptace

- 7.1. Akceptační procedura zahrnuje ověření řádného provedení Díla porovnáním skutečných vlastností Díla s jeho specifikací stanovenou touto Smlouvou a jejími přílohami.
- 7.2. Dodavatel předá dílčí plnění podle Smlouvy nejpozději 10 pracovních dnů před termínem uvedeným v Příloze č. 3 Smlouvy. O řádném předání a převzetí Díla nebo jeho dílčí části bude sepsán předávací protokol s uvedením data předání a převzetí (dále jen „**Předávací protokol**“). Řízení o akceptaci předaného dílčího plnění je zahájeno dnem předání dílčího plnění podle Smlouvy a je ukončeno podpisem akceptačního protokolu Objednatelem a Dodavatelem (dále jen „**Akceptační protokol**“). Objednatel potvrdí příslušný Akceptační protokol pouze v případě, že Dodavatelem předané dílčí plnění splňuje podmínky a vlastnosti stanovené Smlouvou a jejími přílohami, je funkční bez nedodělků a bez vad.
- 7.3. Veškeré zjištěné nedostatky, nedodělky a vady budou Dodavateli kdykoliv po jejich zjištění oznámeny Objednatelem (dále jen „**Oznámení o nedodělcích a vadách**“). Veškeré nedostatky, nedodělky a vady budou Dodavatelem odstraněny bez



zbytečného odkladu po doručení písemného Oznámení o nedodělcích a vadách, a to tak, aby k podpisu příslušného Akceptačního protokolu mohlo dojít v termínu stanoveném pro příslušnou Část Předmětu plnění.

- 7.4. Smluvní strany se mohou dohodnout, že Objednatel převezme plnění, přestože jeho určitá část nesplňuje všechna akceptační kritéria (převzetí s výhradou). Smluvní strany se zároveň dohodnou, do kdy Dodavatel odstraní zbývající vady části plnění tak, aby byla splněna všechna akceptační kritéria, a kdy bude proveden test, který splnění těchto akceptačních kritérií ověří. Tyto skutečnosti budou zaznamenány v Předávacím protokolu vyhotoveném při převzetí plnění s výhradou.
- 7.5. Podpis Akceptačního protokolu s výrokem „akceptováno“ nebo „akceptováno s výhradou“ Objednatelem a Dodavatelem je podmínkou pro vznik oprávnění Dodavatele vystavit fakturu za poskytnutí příslušného dílčího plnění podle této Smlouvy.
- 7.6. Základní akceptační kritéria, včetně akceptační procedury jsou nedílnou součástí Metodiky projektového řízení, která je nedílnou součástí Přílohy č. 5 Smlouvy.

Článek 8.

Práva a povinnosti Smluvních stran

- 8.1. V rámci plnění předmětu Smlouvy mají obě Smluvní strany zejména, nikoliv však výlučně, následující práva a povinnosti:
 - 8.1.1. vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků vyplývajících z této Smlouvy a vzájemně respektovat své oprávněné zájmy související se Smlouvou;
 - 8.1.2. neprodleně informovat druhou Smluvní stranu o vzniku nebo hrozícím vzniku překážky plnění mající významný vliv na řádné a včasné plnění dle této Smlouvy;
 - 8.1.3. poskytovat druhé Smluvní straně úplné, pravdivé a včasné informace o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění dle této Smlouvy;
 - 8.1.4. plnit své závazky vyplývající z této Smlouvy tak, aby nedocházelo k prodlení s plněním jednotlivých termínů a s prodlením splatnosti jednotlivých peněžních závazků;
 - 8.1.5. provést akceptaci Díla případně jeho Částí v souladu s čl. 7 Smlouvy.
- 8.2. V souvislosti s plněním předmětu Smlouvy má Objednatel zejména, nikoliv však výlučně, následující povinnosti:
 - 8.2.1. Vytváření předpokladů pro plnění závazků vyplývajících z této Smlouvy tak, aby mohly být plněny jednotlivé termíny realizace Díla;
 - 8.2.2. poskytování požadovaných podkladů a informací Dodavateli, průběžné zajišťování řádné a včasné spolupráce a součinnosti třetích stran, např. další dotčené subjekty, a to zejména koncoví uživatelé;



- 8.2.3. řádné a včasné předávání potřebných nebo Dodavatelem vyžádaných dokumentů, předpisů, informací, rozhodnutí, specifikací požadavků a dalších podkladů souvisejících s realizací Díla;
- 8.2.4. písemné řádné a včasné vyjadřování se k předkládaným materiálům;
- 8.2.5. poskytování řádné a včasné součinnosti při předávání a akceptacích plnění Díla, resp. jeho dílčího plnění včetně písemného oznamování vad a nedodělků Díla bránících akceptaci Předmětu plnění;
- 8.2.6. poskytování konzultací současného stavu, upřesňování požadavků a zadání v průběhu realizace Díla.
- 8.2.7. zajištění přístupu k produktové podpoře hardware nebo software, která není Předmětem plnění této Smlouvy, pokud této povinnosti nebudou bránit smluvní vztahy uzavřené Objednatelem s třetí stranou, přičemž se v tomto případě zavazuje k maximální součinnosti směřující k zajištění toho přístupu;
- 8.2.8. umožnit Dodavateli přístup do objektů, k zařízení, k programovému vybavení, databázím a informačním systémům Objednatele v rozsahu nezbytném pro řádné plnění této Smlouvy dle vzájemně schválených postupů nebo jeho subdodavatele podílející se na plnění Smlouvy v objektech Objednatele;
- 8.2.9. do 3 dnů ode dne podpisu Smlouvy zajistit jmenování pracovníků Objednatele do všech úrovní Projektu a jejich vybavení pravomocemi potřebnými pro výkon příslušných funkcí v souladu s Přílohou č. 5 Smlouvy. Dále zajištění jejich řádného fungování v rolích jim v rámci Projektu přidělených.
- 8.2.10. Objednatel je oprávněn kontrolovat způsob provádění Díla za účelem ověření souladu s podmínkami stanovenými Smlouvou, zejména pak průběžně konzultovat a schvalovat návrhy Technického projektu.
- 8.3. V souvislosti s plněním předmětu Smlouvy má Dodavatel zejména, nikoliv však výlučně, následující práva a povinnosti:
 - 8.3.1. postupovat při plnění Smlouvy řádně tak, aby bylo dosaženo účelu Smlouvy;
 - 8.3.2. poskytovat Dílo v souladu se sjednanou kvalitou tak, aby vyhovovalo potřebám Objednatele, se kterými byl Dodavatel prokazatelně seznámen;
 - 8.3.3. zajistit dostatečnou kapacitu svých pracovníků, včetně pracovníků subdodavatele s odpovídající kvalifikací pro poskytování Díla;
 - 8.3.4. poskytovat bezplatný záruční servis na Objednatelem reklamované závady po dobu trvání záruční lhůty;
 - 8.3.5. poskytnout jako součást plnění příslušnou kompletní dokumentaci a instalační média, licenční klíče a aktivační kódy k licenčnímu software třetích stran a zdrojové kódy ke všem Autorským dílům, které Dodavatel po dobu platnosti Smlouvy v souladu s čl. 14 Smlouvy poskytne;
 - 8.3.6. poskytovat Objednateli podporu v případě potřeby i e-mailem, faxem nebo dopisem v českém jazyce. Všechny osoby komunikující s pracovníky Objednatele budou schopny se dorozumět, nebude-li dohodou Smluvních stran dohodnuto jinak, v českém jazyce na úrovni rodilých mluvčích;



- 8.3.7. Dodavatel je povinen provádět činnosti podle této Smlouvy s náležitou odbornou péčí a v souladu s platnými obecně závaznými právními předpisy. Dodavatel je rovněž povinen chránit oprávněné zájmy Objednatele, které mu jsou, budou nebo by měly být známy, a postupovat v souladu s příkazy obdrženy od Objednatele;
- 8.3.8. Dodavatel je povinen plnit příkazy Objednatele, přitom je však povinen upozornit Objednatele na nevhodnost jím udělených příkazů nebo případně též na nevhodnou povahu jím poskytnutých věcí, jestliže tuto nevhodnost je schopen zjistit při vynaložení odborné péče;
- 8.3.9. Dodavatel je povinen při plnění povinností dle této Smlouvy aktivně spolupracovat s dalšími dotčenými subjekty specifikovanými v Technickém projektu, a to zejména s koncovými uživateli.

Článek 9.

Součinnost Smluvních stran

- 9.1. Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si součinnost nezbytnou pro řádné plnění předmětu Smlouvy. Smluvní strany jsou povinny informovat bezodkladně druhou Smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění Smlouvy.
- 9.2. V případě prokazatelného prodlení povinné Smluvní strany s poskytnutím součinnosti není oprávněná Smluvní strana v prodlení s plněním svých závazků podle Smlouvy a veškeré lhůty se o prokazatelné prodlení povinné Smluvní strany prodlužují; to neplatí v případech, kdy prodlení v poskytnutí součinnosti ze strany povinné Smluvní strany bylo vyvoláno v přímé příčinné souvislosti s prokazatelným neposkytnutím součinnosti nebo prodlením ze strany oprávněné. Objednatel je v prodlení, jestliže v rozporu se svými povinnostmi vyplývajícími ze smluvního vztahu, nepřevzme řádně nabídnuté bezvadné plnění nebo neposkytne součinnost nutnou k tomu, aby Dodavatel mohl splnit svůj závazek. Dodavatel je v prodlení, jestliže v rozporu se svými povinnostmi vyplývajícími ze smluvního vztahu, nepředá řádné a bezvadné plnění nebo neposkytne součinnost nutnou k tomu, aby Objednatel mohl splnit svůj závazek.
- 9.3. Smluvní strany se zavazují vytvořit pro poskytování součinnosti v rámci svých organizačních struktur optimální komunikační, řídicí a odborné (personální) podmínky.

Článek 10.

Vzájemná komunikace Smluvních stran

- 10.1. Smluvní strany spolu budou komunikovat komunikačními prostředky, kterými jsou zejména email, datová zpráva do datové schránky, písemně v listinné formě i digitálně.
- 10.2. Jména kontaktních osob jsou uvedena v čl. 11 Smlouvy. Smluvní strany jsou oprávněny jimi jmenované kontaktní osoby změnit, přičemž změna je účinná doručením písemného oznámení o takové změně druhé Smluvní straně. Smluvní strany se dohodly, že v případě změny kontaktních osob není nutno ke Smlouvě uzavírat dodatek.



- 10.3. Veškerá oznámení mezi Smluvními stranami, která se vztahují ke Smlouvě, nebo která mají být učiněna na základě Smlouvy a která mají či mohou mít jakýkoliv účinek na trvání, změnu či ukončení této Smlouvy, musí být učiněna v písemné podobě a druhé Smluvní straně doručena buď osobně nebo doporučeným dopisem či jinou formou registrovaného poštovního styku na adresu uvedenou v záhlaví této Smlouvy, není-li Smlouvou stanoveno nebo mezi Smluvními stranami pro konkrétní případy písemně dohodnuto jinak.
- 10.4. Ukládá-li Smlouva doručit některý dokument v písemné podobě, musí být doručen v písemné (listinné) podobě. Se souhlasem Objednatele lze však využít i elektronickou formu (email). Doručování těchto dokumentů musí být v souladu s obecně závaznými právními předpisy.
- 10.5. Oznámením v písemné formě se rozumí doručení oznámení druhé Smluvní straně buď v listinné formě nebo v elektronické (digitální) formě jako dokument ve standardních formátech MS Office nebo *.pdf, nebude-li dohodou Smluvních stran určeno jinak.
- 10.6. Smluvní strany se zavazují, že v případě změny své adresy budou o této změně druhou Smluvní stranu písemně informovat nejpozději do 3 pracovních dnů.

Článek 11.

Základní tým a odpovědné osoby

- 11.1. Osoby oprávněné jednat za Smluvní strany pro jednání smluvní a ekonomická (mimo podpisu Smlouvy a jejích dodatků) a zároveň kontaktními osobami jsou:

za Objednatele:

Jméno a příjmení: Mgr. Bohdan Urban

e-mail: bohdan.urban@mvcrcz

tel: + 420 602 273 273

za Dodavatele:

Jméno a příjmení: Jan Přerovský

e-mail: prerovsky.jan@cpost.cz

tel: + 420 602 337 396

Jméno a příjmení: Petr Solský

e-mail: solsky.petr@cpost.cz

tel: +420 734 518 494



- 11.2. Osoby oprávněné jednat za Smluvní strany pro jednání věcná a technická a zároveň kontaktními osobami jsou:

za Objednatele:

Jméno a příjmení: Ing. Monika Syrovátková

e-mail: monika.syrovatkova@mvcr.cz

tel: +420 607 697 459

Jméno a příjmení: Ing. Nika Metzová

e-mail: nika.metzova@mvcr.cz

tel: +420 728 118 407

za Dodavatele:

Jméno a příjmení: Jan Mikulecký

e-mail: mikulecky.jan@cpost.cz

tel: +420 603 451 764

Jméno a příjmení: Vladimír Příbramský

e-mail: pribramsky.vladimir@cpost.cz

tel: +420 603 190 714

Článek 12.

Záruky

- 12.1. Dodavatel je povinen se seznámit se všemi informacemi, které souvisí s předmětem Smlouvy nebo mu byly v souvislosti s ní poskytnuty Objednatelem. Pokud by některé informace nebyly dostatečné, aby dovolily řádné dodání Předmětu plnění, je povinností Dodavatele si zajistit chybějící informace. Dodavatel odpovídá za chybné či nepřesné informace v dílčím plnění, existující v době jeho předání. Neodpovídá za chyby způsobené použitím nevhodných podkladů poskytnutých Objednatelem, pokud však Dodavatel na tyto nevhodné podklady písemně upozornil a Objednatel na jejich použití i přes písemné upozornění Dodavatelem trval.
- 12.2. Dodavatel odpovídá za to, že Dílo bude fungovat v souladu s požadavky Objednatele uvedenými ve Smlouvě, jejích přílohách a v Technickém projektu. Dodavatel v souvislosti s odpovědností za vady Díla a jeho dílčích částí poskytuje Objednateli záruku následovně:
- 12.2.1. Dodavatel Objednateli garantuje záruku po dobu minimálně 36 měsíců ode dne dodání HW komponent Díla, a že nahradí nebo obnoví funkčnost jakékoliv části



vykazující vadu nebo chovající se v rozporu s technickou dokumentací v termínech dle Přílohy č. 5 Smlouvy;

- 12.2.2. Dodavatel Objednateli garantuje po dobu minimálně 12 měsíců ode dne dodání platformního SW, že poskytne všechny nové verze, meziverze, záplaty či jednorázové opravy včetně veškerých užívacích nevýhradních časově neomezených práv v rozsahu stanoveném Smlouvou či Technickým projektem ke všem dodaným licencím SW produktů;
- 12.2.3. Dodavatel v souvislosti s odpovědností za vady Díla poskytuje Objednateli na Dílo s výjimkou HW a SW komponent uvedených v odst. 12.2.1 a 12.2.2 záruku, a to po dobu minimálně 24 měsíců od akceptace poslední části Díla. Dodavatel se zavazuje odstranit vady Díla, jež bude mít Dílo v době jeho předání Objednateli a dále vady, které se na Díle vyskytnou v průběhu záruční doby. Tato záruka se nevztahuje na provozní incidenty.
- 12.3. Záruka dle čl. 12.2 této Smlouvy poskytovaná Dodavatelem se vztahuje na všechny Části Díla včetně jeho příslušenství, na funkčnost Díla, jakož i na jeho vlastnosti požadované Objednatelem. Záruční doba se prodlužuje o dobu, po kterou mělo Dílo vadu bránící jeho řádnému užívání Objednatelem.
- 12.4. Veškeré zjištěné nedostatky, nedodělky a vady Díla, které se vyskytnou v záruční době, se Dodavatel zavazuje po jejich oznámení Objednatelem Dodavateli odstranit, a to ve lhůtách v souladu s Přílohou č. 5 Smlouvy.
- 12.5. Práva a povinnosti Smluvních stran uvedená v tomto článku trvají, za podmínek v tomto článku uvedených, i po ukončení této Smlouvy.
- 12.6. Vady budou kontaktními osobami Objednatele hlášeny Dodavateli komunikačními prostředky v souladu s čl. 10.1 Smlouvy. Kategorie vad jsou definovány v Příloze č. 5 této Smlouvy.

Článek 13.

Schvalování Technického projektu

- 13.1. Dodavatel musí při návrhu a realizaci Technického projektu respektovat ustanovení této Smlouvy. Dodavatel je povinen předložit Objednateli takový návrh Technického projektu, který je plně v souladu se Smlouvou. Současně Objednatel nebude akceptovat takový Technický projekt, který není v souladu se Smlouvou. Po akceptaci Technického projektu Objednatelem se Technický projekt stane plně závazným dokumentem pro Smluvní strany.
- 13.2. Dodavatel bude v rámci konzultací Technického projektu předávat Objednateli i návrh budoucích nákladů na provoz, dohled a údržbu řešení navrženého Technickým projektem. Objednatel má právo řešení navržené Technickým projektem odmítnout v případě, že má důvodné pochybnosti o naplnění cílů vytvoření Dohledového centra SOCCR. V takovém případě je Dodavatel povinen bez zbytečného odkladu na vlastní náklady změnit technické řešení Projektu tak, aby bylo dosaženo všech cílů vytvoření Dohledového centra SOCCR.



13.3. V případě změny detailu technického projektu („ZDTP“) se nejedná o změnové řízení Projektu, tak, jak je definováno Příloze č. 5 Smlouvy, ale o drobné odchylky v detailech technického řešení oproti schválenému Technickému projektu (bez změny ceny Díla). Mechanismus schvalování ZDTP bude následující:

- popis a zdůvodnění změny,
- návrh řešení,
- schválení změny.

13.4. Schválení ZDTP proběhne na jednání schvalovací komise, která bude složena ze zástupců obou Smluvních stran. Komise na tomto jednání ZDTP:

- schválí,
- zamítne,
- vrátí k dopracování, pokud vzniknou pochybnosti např. o návrhu řešení.

O ZDTP bude sepsán „Změnový Protokol“, který podepíší obě Smluvní strany. Dodavatel navrhne proces změnového řízení a formulář Změnového protokolu.

Článek 14.

Autorské a vlastnické právo

14.1. Pokud při realizaci předmětu plnění dle této Smlouvy vznikne plnění, které naplňuje znaky autorského díla ve smyslu Autorského zákona, poskytuje Dodavatel Objednateli a Objednatel od Dodavatele získává práva související s ochranou duševního vlastnictví vztahující se k takovému dílu v rozsahu nezbytném pro řádné užívání všech autorských děl, které jsou součástí Předmětu plnění dle této Smlouvy (dále jen „**Autorská díla**“). Objednatel zejména získává od Dodavatele oprávnění k výkonu práva užití Autorská díla, a to vždy ke dni dokončení akceptačního řízení, na jehož základě dochází k dodání dílčího plnění dle Smlouvy, jehož součástí je příslušné Autorské dílo. Oprávnění k výkonu práva užití výše uvedená Autorská díla jsou poskytována Dodavatelem Objednateli, pokud nebude dohodnuto jinak, formou licenčního ujednání ve smyslu ustanovení § 2358 a násl. Občanského zákoníku majícího následující charakteristiky:

- 14.1.1. výhradní licence k veškerým známým způsobům užití jednotlivých Autorských děl a jejich případných dalších verzí, zejména k účelu, ke kterému bylo takové dílo Dodavatelem vytvořeno v souladu se Smlouvou, a to v rozsahu minimálně nezbytném pro řádné užívání předmětu plnění dle této Smlouvy Objednatelem,
- 14.1.2. licence neomezená územním či množstevním rozsahem a rovněž tak neomezená rozsahem užití, zejména neomezená počtem uživatelů či mírou využívání,
- 14.1.3. licence udělená na dobu určitou, a to po celou dobu trvání majetkových práv k předmětným Autorským dílům,
- 14.1.4. licence převoditelná a postupitelná, tj. která je udělena s právem udělení podlicence či postoupení licence jakékoliv třetí osobě,



- 14.1.5. Dodavatel prohlašuje, že cena za veškerá oprávnění a plnění poskytnutá Objednateli a dalším osobám v souladu s tímto článkem Smlouvy je již zahrnuta v ceně za poskytnuté plnění dle Smlouvy.
- 14.1.6. V případě, že při realizaci předmětu plnění dojde k použití standardizovaných softwarových produktů třetích stran, u kterých není obvyklé a u kterých nelze po Dodavateli spravedlivě požadovat, aby poskytl k takovým Autorským dílům a databázím licenci a související oprávnění v souladu s požadavky uvedenými v odstavci 14.1.1. až 14.1.4. tohoto článku, se tato ustavení Smlouvy neuplatní. V případě těchto Autorských děl a databází je Dodavatel povinen zajistit, že bude oprávněnou osobou uděleno Objednateli nevýhradní oprávnění k výkonu práva užít díla tvořící tento software a k výkonu práva vytěžovat a zužítkovat databáze tvořící tento software, a to v územním rozsahu zahrnujícím minimálně celé území České republiky a všemi způsoby odpovídajícími účelu, pro který jsou takové Autorské dílo a databáze určeny. Poskytnutí zdrojových kódů není v případě takových Autorských děl vyžadováno.
- 14.2. Ve vztahu k Autorským dílům majících povahu software, s výjimkou ustanovení odst. 14.1.6., je Dodavatel povinen předat Objednateli zdrojový kód a veškeré související materiály (zejm. kompletní specifikace, příručky, pracovní dokumenty) v editovatelné elektronické podobě, a to nejpozději ke dni ukončení relevantního Akceptačního řízení. Na základě výzvy Objednatele je Dodavatel povinen poskytovat Objednateli nebo Objednatelem určené třetí osobě bezplatně konzultace k veškerým zdrojovým kódům předaným dle této Smlouvy a to po dobu trvání záruční doby dle této Smlouvy.
- 14.2. S výhradou případného odlišného ujednání Smluvních stran uděluje Dodavatel Objednateli souhlas k tomu, aby nejpozději ke dni poslední akceptace Předmětu plnění dle této Smlouvy byl Objednatel oprávněn jednotlivá Autorská díla zveřejnit, upravovat, zpracovávat, překládat, či měnit jejich název, a že je též oprávněn tato Autorská díla spojit s dílem jiným a zařadit je do díla souborného. Dodavatel uděluje Objednateli souhlas k tomu, aby Objednatel svěřil svá práva dle tohoto článku Smlouvy třetím osobám, které budou v budoucnu užívat Autorská díla vznikuvší na základě této Smlouvy.
- 14.3. Vznikne-li v rámci předmětu plnění dle této Smlouvy plnění naplňující znaky databáze dle Autorského zákona, pak Dodavatel k okamžiku pořízení databáze poskytuje Objednateli zvláštní právo pořizovatele databáze, a to zejména právo databázi vytěžovat i zužítkovávat, a to jak celý její obsah, tak i její kvalitativně nebo kvantitativně podstatné části. Dodavatel dále poskytuje Objednateli právo udělit oprávnění k výkonu práva pořizovatele databáze jinému subjektu v rozsahu, jak je udělil Dodavatel Objednateli.
- 14.4. Dodavatel prohlašuje, že udělení veškerých práv uvedených v tomto článku Smlouvy nelze ze strany Dodavatele vypovědět a že na udělení těchto práv nemá vliv ani případné ukončení platnosti Smlouvy. Budou-li v budoucnu splněny podmínky pro odstoupení Dodavatele pro nečinnost nabyvatele licence dle ustanovení § 2378 odst. 1 a 2 Občanského zákoníku, nemůže Dodavatel uplatnit právo na odstoupení



od Smlouvy před uplynutím 10 let ode dne závěrečné akceptace předmětu plnění dle této Smlouvy.

- 14.5. Dodavatel zároveň prohlašuje, že užitím Autorských děl a databází Objednatel v souladu s touto Smlouvou nejsou dotčena autorská ani jiná práva třetích osob. Dodavatel odpovídá Objednateli za škodu, která by vznikla Objednateli v důsledku uplatnění práv duševního vlastnictví třetích osob vůči Objednateli pro řádné užívání Autorských děl nebo databází, k němuž udělil nebo zajistil Dodavatel licenci či podlicenci na základě tohoto článku Smlouvy. Dodavatel se tímto zavazuje poskytnout Objednateli na svůj náklad veškerou účinnou součinnost nutnou pro úspěšnou obranu práv Objednatele ve vztahu k uplatnění práv duševního vlastnictví třetích osob. Objednatel se zavazuje bez zbytečného odkladu oznámit Dodavateli, že došlo k uplatnění nároků třetích osob pro porušování jejich práv duševního vlastnictví v souvislosti s plněním dle této Smlouvy.

Článek 15.

Odpovědnost za škodu

- 15.1. Každá ze Smluvních stran nese odpovědnost za škodu způsobenou v důsledku porušení povinností vyplývajících z obecně závazných právních předpisů či vyplývajících z této Smlouvy. Obě Smluvní strany se zavazují vyvíjet maximální úsilí k předcházení škodám a k minimalizaci vzniklých škod.
- 15.2. Dodavatel odpovídá za škodu vzniklou Objednateli v souvislosti s plněním, nedodržením nebo porušením povinností Dodavatele vyplývajících z této Smlouvy nebo v souvislosti s provozní činností Dodavatele.
- 15.3. Žádná ze Smluvních stran neodpovídá za škodu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé Smluvní strany. Ustanovení čl. 8.3.8 Smlouvy tím není dotčeno. Žádná ze Smluvních stran dále neodpovídá za škodu vzniklou nesplněním závazku zapříčiněným výlučně v důsledku prodlení druhé Smluvní strany. Důvody pro vyloučení odpovědnosti za škodu se shodně uplatní také jako případy, ve kterých nevzniká Smluvní straně nárok na smluvní pokutu.
- 15.4. Žádná Smluvní strana není povinna k náhradě škody, prokáže-li, že jí ve splnění povinnosti ze Smlouvy dočasně nebo trvale zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na její vůli ve smyslu ustanovení § 2913 odst. 2 Občanského zákoníku. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání výše uvedených překážek.
- 15.5. Za mimořádnou nepředvídatelnou a nepřekonatelnou překážkou vzniklou nezávisle na vůli smluvní strany ve smyslu ustanovení § 2913 odst. 2 Občanského zákoníku se považují zejména válka, ozbrojený konflikt, embargo, občanské nepokoje, sabotáže, teroristické činy nebo hrozba sabotáže či teroristického činu, epidemie, výbuchy, chemická nebo radioaktivní kontaminace nebo ionizující záření, zásahy bleskem, zemětřesení, vánice, povodně, požáry, vichřice, bouře nebo jiné působení přírodních živlů, uzavření podniků nebo jiné kroky v rámci průmyslových odvětví nebo, srážky nebo působení vozidel, letadel nebo předmětů padajících z letadel nebo jiných



vzdušných zařízení nebo výskyt tlakových vln způsobených letadly či jinými vzdušnými zařízeními pohybujícími se nadzvukovou rychlostí, a dále také řízení vedené u Úřadu pro ochranu hospodářské soutěže s výjimkou případů, kdy Úřad (či odvolací orgán) konstatuje porušení práv a povinností Dodavatele vyplývající ze zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů (dále jen „**Zákon o veřejných zakázkách**“), či podání námitek stěžovatele ve smyslu ustanovení § 110 Zákona o veřejných zakázkách, s výjimkou případů, kdy v následném řízení Úřad (či odvolací orgán) konstatuje porušení práv a povinností Dodavatele vyplývající ze Zákona o veřejných zakázkách.

- 15.6. Brání-li některé ze Smluvních stran v plnění povinností ze Smlouvy mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na její vůli ve smyslu ustanovení § 2913 odst. 2 Občanského zákoníku, je Smluvní strana povinna o vzniku, důsledcích, povaze a zániku takové překážky Objednatele neprodleně informovat. Zpráva musí být podána písemně, neprodleně poté, kdy se povinná Smluvní strana o překážce dozvěděla, nebo při náležitě péči mohla dozvědět. Bezprostředně po zániku takové překážky povinná Smluvní strana obnoví plnění svých závazků vůči druhé Smluvní straně a učiní vše, co je v jejích silách, ke kompenzaci doby, která uplynula v důsledku takového prodlení.
- 15.7. Pokud překážka nepomine do 3 pracovních dnů od doby svého vzniku, oprávnění zástupci obou Smluvních stran se sejdou za účelem projednání dalšího postupu při plnění závazků vyplývajících ze Smlouvy.
- 15.8. Škody, které prokazatelně vzniknou v souvislosti s činností Dodavatele či Objednatele dle této Smlouvy, se Smluvní strany zavazují zaplatit druhé Smluvní straně na základě samostatné faktury.
- 15.9. Dodavatel se zavazuje, že vytvoření a realizace Dohledového centra SOCCR, nenaruší realizaci, financování ani chod projektů CMS, ITS NGN, NIS IZS a KSP. V případě, že Dodavatel svou činností při vytváření Dohledového centra SOCCR dle této Smlouvy naruší financování, realizaci a chod některého z projektů CMS, ITS NGN, NIS IZS nebo KSP, odpovídá Dodavatel Objednateli za škodu takto způsobenou, pokud byla prokazatelně způsobena činností Dodavatele.
- 15.10. Smluvní strany se zavazují, že vždy před uplatněním nároku na náhradu škody písemně vyzvou povinnou Smluvní stranu k jednání o způsobu stanovení výše škody, a to bez zbytečného odkladu poté, kdy se oprávněná Smluvní strana prokazatelně dozví o vzniku škodní události.

Článek 16.

Sankce

- 16.1. V případě prodlení Dodavatele s dodáním Předmětu plnění nebo jeho Části v termínu podle harmonogramu obsaženého v Příloze č. 3 Smlouvy, má Objednatel vůči Dodavateli právo na smluvní pokutu ve výši 0,05 % z ceny Části Předmětu plnění bez DPH, kde došlo k prodlení, za každý, i započatý, den prodlení, maximálně však do výše ceny Části Předmětu plnění, při jejímž poskytování Dodavatel porušil povinnost, která byla příčinou pro vznik nároku na smluvní pokutu.



- 16.2. Za prodlení Objednatele s úhradou faktury má Dodavatel vůči Objednateli právo na smluvní pokutu ve výši 0,05 % z dlužné částky bez DPH za každý, i započatý, den prodlení po termínu splatnosti, maximálně však do výše hodnoty dlužné fakturované částky, s jejíž úhradou je Objednatel v prodlení.
- 16.3. V případě, že Dodavatel poruší povinnost uvedenou v článku 6 odst. 6.11 Smlouvy, je Objednatel oprávněn požadovat smluvní pokutu ve výši duplicitně fakturované částky.
- 16.4. Pro jeden případ porušení povinností stanovených touto Smlouvou nelze kumulativně uplatnit více smluvních pokut. Vznikem povinnosti platit smluvní pokutu ani jejím faktickým zaplacením není dotčeno právo poškozeného na náhradu škody ani právo odstoupit od Smlouvy. Odstoupením od Smlouvy nárok na již uplatněnou smluvní pokutu nezaniká.
- 16.5. V případě, že Dodavatel neodstraní záruční vady Díla specifikované Příloze č. 5 Smlouvy v termínech dle Přílohy č. 5 Smlouvy, je povinen Objednateli uhradit smluvní pokutu, a to ve výši:
- a) 50.000,- Kč bez DPH za každé jednotlivé nedodržení výše uvedeného termínu v případě neodstranění vady s prioritou požadavku 1 - kritická, a to za každou i započatou hodinu prodlení,
 - b) 25.000,- bez DPH za každé jednotlivé nedodržení výše uvedeného termínu v případě neodstranění vady s prioritou požadavku 2 - vysoká, a to za každou i započatou hodinu prodlení,
 - c) 20.000,- Kč bez DPH za každé jednotlivé nedodržení výše uvedeného termínu v případě neodstranění vady s prioritou požadavku 3 - střední, a to za každý i započatý den prodlení
 - d) 10.000,- Kč bez DPH za každé jednotlivé nedodržení výše uvedeného termínu v případě neodstranění vady s prioritou požadavku 4 - nízká, a to za každý i započatý den prodlení
- Úhrnná smluvní pokuta udělená Objednatelem Dodavateli dle čl. 16 odst. 16.5. Smlouvy činí v součtu nejvíce 5% z ceny Díla za jeden kalendářní rok.
- Dodavatel dále odpovídá Objednateli za případnou škodu, která mu vznikne z titulu neodstranění vad Díla specifikovaných v Příloze č. 5 Smlouvy Dodavatelem v termínech dle Přílohy č. 5 Smlouvy.
- 16.6. Vznikem povinnosti platit smluvní pokutu ani jejím skutečným zaplacením nezaniká povinnost Smluvních stran splnit povinnost, jejíž plnění bylo zajištěno smluvní pokutou.
- 16.7. Smluvní pokuty jsou splatné do 30 kalendářních dnů po obdržení vyúčtování smluvní pokuty na základě samostatné faktury. Pokud bude takto vystavená faktura doručena Objednateli v období mezi 16. prosincem a 28. únorem příslušného kalendářního roku, Smluvní strany se dohodly, že na žádost Objednatele Dodavatel prodlouží splatnost faktury na 60 kalendářních dní ode dne doručení.
- 16.8. Žádná ze Smluvních stran není povinna zaplatit smluvní pokutu, pokud prokáže, že porušení povinností bylo způsobeno mimořádnou nepředvídatelnou a nepřekonatelnou překážkou vzniklou nezávisle na vůli Smluvní strany ve smyslu § 2913 odst. 2 Občanského zákoníku.



Článek 17.

Ustanovení o vzniku a zániku Smlouvy

- 17.1. Smlouva nabývá platnosti a účinnosti dnem jejího uzavření. Dnem uzavření Smlouvy je den označený datem u podpisů Smluvních stran. Je-li takto označeno více dní, je dnem uzavření Smlouvy den z označených dnů nejpozdější.
- 17.2. Smlouva může být zrušena dohodou Smluvních stran v písemné formě, přičemž účinky zrušení Smlouvy nastanou k okamžiku stanovenému v takovéto dohodě. Nebude-li takovýto okamžik dohodou stanoven, pak tyto účinky nastanou ke dni účinnosti takovéto dohody.
- 17.3. Za podstatné porušení Smlouvy Dodavatelem, které zakládá právo Objednatele na odstoupení od Smlouvy, se považuje zejména
 - 17.3.1. neodstranění vad Díla ve lhůtě stanovené ve Smlouvě;
 - 17.3.2. porušení jakékoliv povinnosti Dodavatele dle Smlouvy;
 - 17.3.3. nepravdivost jakéhokoli prohlášení uvedeného v čl. 19.2. Smlouvy;
 - 17.3.4. porušení povinnosti Dodavatele při provádění Díla v případě, že na porušení povinnosti byl Objednatelem písemně upozorněn a Dodavatel ani po tomto upozornění neprovedl v přiměřené době stanovené Objednatelem nápravu a neprováděl Dílo řádných způsobem;
 - 17.3.5. postup Dodavatele v rozporu s příkazy Objednatele.
- 17.4. Objednatel je dále oprávněn od této Smlouvy odstoupit v případě, že
 - 17.4.1. vůči majetku Dodavatele probíhá insolvenční řízení, v němž bylo vydáno rozhodnutí o úpadku, pokud to právní předpisy umožňují;
 - 17.4.2. insolvenční návrh na Dodavatele byl zamítnut proto, že majetek Dodavatele nepostačuje k úhradě nákladů insolvenčního řízení;
 - 17.4.3. Dodavatel vstoupí do likvidace;
 - 17.4.4. Dodavatel pozbude jakékoli oprávnění vyžadované právními předpisy pro provádění činností, k nimž se podle Smlouvy zavazuje;
 - 17.4.5. Dodavatel nedodrží při plnění Smlouvy relevantní právní předpisy, technické normy, dokumentaci schválenou Objednatelem nebo podmínky rozhodnutí orgánů státní správy či samosprávy;
 - 17.4.6. Dodavatel bude v prodlení se splněním své povinnosti, které bude znamenat podstatné porušení jeho smluvní povinnosti, a to i přesto, že na toto prodlení bude Objednatelem písemně upozorněn a nezjedná nápravu v dodatečně poskytnuté přiměřené lhůtě.
- 17.5. Objednatel je oprávněn po předání Části 1 Předmětu plnění a po předchozím projednání s Dodavatelem, od Smlouvy odstoupit.
- 17.6. Dodavatel je oprávněn od Smlouvy odstoupit v případě, že Objednatel bude v prodlení s úhradou svých peněžitých závazků vyplývajících z této Smlouvy po dobu delší než šedesát (60) kalendářních dní.
- 17.7. Odstoupení od Smlouvy musí mít písemnou formu, přičemž písemný projev vůle odstoupit od Smlouvy musí být druhé Smluvní straně doručen.



- 17.8. Účinky odstoupení od Smlouvy nastanou okamžikem doručení písemného projevu vůle odstoupit od Smlouvy druhé Smluvní straně. Smluvní strany se dohodly, že nebudou mít povinnost vrátit si plnění, které již bylo akceptováno před odstoupením od Smlouvy.
- 17.9. Odstoupení od Smlouvy se nedotýká práva na náhradu škody vzniklé porušením Smlouvy a právních předpisů nebo práva na zaplacení smluvní pokuty.

Článek 18.

Zvláštní ujednání

- 18.1. Dodavatel je povinen v případě zadávání veřejných zakázek souvisejících s realizací plnění dle této Smlouvy postupovat v souladu se Zákonem o veřejných zakázkách, a veškerou dokumentaci, která souvisí se zadáním veřejné zakázky postupem dle výše uvedeného zákona předložit Objednateli, a to do 15 kalendářních dnů od každého jednotlivého úkonu Dodavatele v rámci zadávání veřejné zakázky. Dodavatel je povinen předložit nabídku vítězného uchazeče Objednateli ke kontrole, a to před uzavřením smlouvy s tímto uchazečem. Bez písemného souhlasu Objednatele není Dodavatel oprávněn smlouvu s vybraným uchazečem o veřejnou zakázku uzavřít. Dále je Dodavatel povinen předložit Objednateli nabídky ostatních uchazečů, bude-li k tomu Objednatelem vyzván. Objednatel je povinen vyjádřit svůj souhlas či nesouhlas s uzavřením smlouvy s vybraným uchazečem nejpozději do 5 pracovních dnů od předložení nabídky vítězného uchazeče Objednateli ke kontrole. Vysloví-li Objednatel s uzavřením smlouvy s vybraným uchazečem nesouhlas, je povinen sdělit Dodavateli důvody takového vyjádření. Toto ustanovení ve vztahu k předkládání dokumentace Objednateli se neaplikuje v případě, že OSF již provedl kontrolu dokumentů souvisejících se zadávacím řízením v rámci projektů CMS, ITS NGN, KSP a NIS IZS.
- 18.2. Pokud Objednatel vyzve Dodavatele k poskytnutí plnění uvedených v této Smlouvě, zavazuje se Dodavatel před zahájením poskytování takového plnění prověřit, zdali takové plnění zcela nebo zčásti nespadá do předmětu plnění jiných platných a účinných smluvních závazků uzavřených mezi Dodavatelem a Objednatelem. O výsledcích uvedené prověrky se Dodavatel zavazuje Objednatele písemně vyznat bezodkladně po jejím ukončení. Před skončením uvedené prověrky a podáním informace Objednateli o jejím výsledku není Dodavatel oprávněn zahájit poskytování plnění uvedených v této Smlouvě.
- 18.3. Jakékoliv informace a výstupy získané v souvislosti s plněním jiných platných a účinných smluvních závazků, uzavřených mezi Dodavatelem a Objednatelem, které jsou využitelné pro plnění Předmětu plnění dle této Smlouvy, je Dodavatel povinen bezplatně poskytnout Objednateli a současně je použit při poskytování Předmětu plnění dle této Smlouvy.
- 18.4. Dodavatel se zavazuje, že naplněním předmětu Plnění této Smlouvy dojde k naplnění požadavků technických opatření dle ZoKB a všech souvisejících platných prováděcích právních předpisů. Technický projekt, který je předmětem Části 1 Předmětu plnění dle této Smlouvy, popíše způsob a rozsah zajištění procesních a technických požadavků provozních dohledů pro systémy ITS NGN, KSP, NIS IZS, včetně popisu dalšího



potřebného rozvoje provozních dohledů těchto systémů, který není financován v rámci dodávky tohoto Předmětu plnění.

Článek 19. Prohlášení Dodavatele

- 19.1. Dodavatel bere na vědomí, že Objednatel při uzavírání Smlouvy bere mimo jiné v úvahu rozsah a pravdivost níže uvedených prohlášení Dodavatele.
- 19.2. Dodavatel tímto prohlašuje, že ke dni uzavření Smlouvy:
 - 19.2.1. Předmětem činnosti Dodavatele je výkon vybraných služeb na základě Zakládací listiny ze dne 16. 12. 1997 ve znění pozdějších dodatků, zejména služeb informačních a komunikačních technologií využívaných státní správou a tyto služby poskytuje výhradně státní správě, nikoliv soukromým subjektům.
 - 19.2.2. Dodavatel v současné době vykonává podstatnou část své činnosti ve prospěch zakladatele státního podniku, tj. Objednatele, spočívající zejména v poskytování vybraných služeb informačních a komunikačních technologií.
 - 19.2.3. Dodavatel je s Objednatelem oprávněn uzavírat Smlouvy mimo režim Zákona o veřejných zakázkách, a to i například na základě aplikace obecné výjimky z působnosti Zákona o veřejných zakázkách, uvedené v ustanovení § 18 odst. 1 písm. e) tohoto zákona, která stanoví, že zadavatel není povinen zadávat podle zákona ty veřejné zakázky, jestliže jejich předmětem je poskytnutí dodávek, služeb nebo stavebních prací veřejnému zadavateli osobou, která vykonává podstatnou část své činnosti ve prospěch tohoto veřejného zadavatele a ve které má veřejný zadavatel výlučná majetková práva; veřejný zadavatel má výlučná majetková práva v určité osobě, zejména pokud disponuje sám veškerými hlasovacími právy plynoucími z účasti v takové osobě nebo pokud taková osoba má právo hospodařit s majetkem veřejného zadavatele, nemá vlastní majetek a výlučně veřejný zadavatel vykonává kontrolu nad hospodařením takové osoby;
 - 19.2.4. Celková cena za realizaci Předmětu plnění odpovídá tržnímu prostředí České republiky v odvětví informačních a komunikačních technologií a jedná se o cenu v daném místě a v čase obvyklou;
 - 19.2.5. Dodavatel má nezbytná schválení jednotlivých orgánů Dodavatele, popř. jiných subjektů a je právně způsobilý k uzavření Smlouvy a k realizaci plnění zamýšleného Smlouvou, a to za podmínek dle Smlouvy, a že osoby podepisující Smlouvu jménem nebo za Dodavatele jsou k tomuto řádně oprávněny;
 - 19.2.6. Dodavatel není v platební neschopnosti a podle nejlepšího vědomí Dodavatele neprobíhají žádná řízení týkající se likvidace, úpadku, exekuce, prodeje podniku Dodavatele nebo jeho části nebo jiná řízení ve smyslu zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení, ve znění pozdějších předpisů (dále jen „Insolvenční zákon“) včetně smírčího řízení, insolvenčního řízení nebo ujednání s věřiteli ve vztahu k likvidaci, exekuci, prodeji podniku nebo části podniku nebo jiné řízení o úpadku ve vztahu k Dodavateli a podle nejlepšího vědomí Dodavatele nebyly podniknuty žádné kroky k vynucení



jakéhokoliv zajištění majetku Dodavatele a nedošlo k žádné události, která by zakládala právo takové zajištění vynucovat;

- 19.2.7. Dodavatel je na základě veškerých nezbytných úkonů, které učinil, řádně a platně oprávněn k tomu, aby uzavřel a plnil Smlouvu po celou dobu její účinnosti, a pokud Smlouva výslovně nestanoví jinak, nebude za tímto účelem nutný žádný souhlas, zproštění, schválení, licence, jmenování ani oprávnění či jakékoli prohlášení, oznámení o učinění podání jakékoli osobě nebo instituci, a nezakládá se tím ani nebude založeno žádné porušení ujednání či dohody, rozsudků, rozhodčích nálezů a právních předpisů, kde je Dodavatel jednou ze stran nebo jimiž je vázán Dodavatel či jakákoliv část jeho majetku;
- 19.2.8. Dodavatel prohlašuje, že plněním Smlouvy nebudou porušena práva třetích osob, z nichž by pro Objednatele vyplynul finanční nebo jiný závazek ve prospěch třetí strany. V případě porušení tohoto závazku je Dodavatel v plném rozsahu odpovědný za případné následky takového jednání;
- 19.2.9. Dodavatel se zavazuje udržívat v platnosti po celou dobu plnění závazků ze Smlouvy pojištění odpovědnosti za škodu způsobenou Dodavatelem třetí osobě. Dodavatel je povinen předložit kopii pojistné smlouvy na vyžádání Objednateli;
- 19.2.10. Dodavatel má schopnost zajistit komplexní provoz sdílených služeb od provozu ICT infrastruktury po zajištění všech provozních a obchodních procesů a prostřednictvím moderních logistických služeb má schopnost zajistit služby s přidanou hodnotou, které dále zefektivní zajišťované služby;
- 19.2.11. Dodavatel má silnou technologickou kompetenci se zaváděním a provozem IS s celostátní působností;
- 19.2.12. Dodavatel disponuje rozsáhlou regionální sítí servisních ICT techniků pokrývající celé území České republiky a má silnou kompetenci v oblasti centralizovaných nákupních procesů a má schopnost zajistit administraci celého zadávacího procesu, od analýzy poptávaných komodit, administraci předmětného zadávacího řízení, po zajištění distribuce;
- 19.2.13. Smlouva představuje platný a právně závazný závazek Dodavatele, který je vůči Dodavateli vynutitelný v souladu s podmínkami Smlouvy;
- 19.2.14. Dodavatel se detailně seznámil s rozsahem a povahou Díla, jsou mu známy veškeré technické, kvalitativní a jiné podmínky předané Objednatelem, a disponuje takovými kapacitami a odbornými znalostmi, které jsou nezbytné pro realizaci Předmětu plnění dle Smlouvy za cenu uvedenou ve Smlouvě;
- 19.2.15. Dodavatel ke dni uzavření Smlouvy splňuje veškeré požadavky uvedené v oddíle VII Statutu státního podniku Česká pošta, s.p. a dále veškeré požadavky uvedené v příloze č. 3 Organizačního řádu České pošty, s.p. označené Pravidla organizace, činnosti a hospodaření Odštěpného závodu ICT služby, ve znění platném ke dni uzavření Smlouvy. V případě, že během trvání závazků založených Smlouvou dojde ke změně přílohy č. 3 Organizačního řádu České pošty, s.p., je pro posouzení dodržení závazků Dodavatele rozhodující



znění této přílohy platné ke dni uzavření Smlouvy, ledaže Objednatel dal výslovný písemný souhlas se změnou tohoto dokumentu. V případě, že během trvání závazků založených Smlouvou dojde ke změně Statutu státního podniku Česká pošta, s.p., je pro posouzení dodržení závazků Dodavatele rozhodující nové znění tohoto dokumentu, a to ode dne účinnosti provedené změny.

- 19.3. V případě, že se jakékoliv prohlášení Dodavatele dle této Smlouvy ukáže jako nepravdivé, má se za to, že Dodavatel v takovém případě porušil tuto Smlouvu podstatným způsobem, přičemž Dodavatel dále nahradí Objednateli veškerou škodu nebo újmu, která Objednateli vznikne v důsledku takového stavu.
- 19.4. Dodavatel se zavazuje vyvinout úsilí, které lze spravedlivě požadovat, pro to, aby prohlášení Dodavatele dle Smlouvy zůstala pravdivá a v platnosti po celou dobu účinnosti této Smlouvy. Objednatel je oprávněn Dodavatelem ve Smlouvě prohlašované skutečnosti nezávisle ověřit a/nebo požádat Dodavatele, aby zdarma poskytl Objednateli doklad potvrzující tvrzené skutečnosti.

Článek 20.

Závěrečná ustanovení

- 20.1. Právní vztahy výslovně Smlouvou neupravené se řídí relevantními ustanoveními Občanského zákoníku.
- 20.2. Smluvní strany prohlašují, že předmětem této Smlouvy není zajištění rozvoje, provozu a souvisejících servisních úkonů Díla; za tímto účelem se zavazují uzavřít nejpozději do akceptace (podpisu akceptačního protokolu) 2. části Předmětu plnění servisní smlouvu.
- 20.3. Obě Smluvní strany prohlašují, že skutečnosti uvedené ve Smlouvě nepovažují za obchodní tajemství ve smyslu ustanovení § 504 Občanského zákoníku a udělují svolení k jejich užití a zveřejnění bez stanovení jakýchkoliv dalších podmínek, zejména dle ustanovení § 147a Zákona o veřejných zakázkách.
- 20.4. Všechny spory, které vzniknou ze Smlouvy nebo v souvislosti s ní a které se nepodaří vyřešit přednostně smírnou cestou, budou rozhodovány obecnými soudy v souladu s ustanoveními zákona č. 99/1963 Sb., občanského soudního řádu, ve znění pozdějších předpisů.
- 20.5. Právní účinky doručení jakékoli písemnosti doručované v souvislosti se Smlouvou či na jejím základě nastávají pouze tehdy, je-li tato písemnost odesílatelem či odesílatelem pověřeným provozovatelem poštovních služeb osobně předána jejímu adresátovi nebo je-li tato písemnost doručena jejímu adresátovi formou doporučeného psaní odeslaného prostřednictvím držitele poštovní licence nebo zvláštní poštovní licence ve smyslu zákona č. 29/2000 Sb., o poštovních službách, ve znění pozdějších předpisů. Při doručování prostřednictvím osobního předání nastávají účinky doručení okamžikem písemného potvrzení adresáta o přijetí doručované písemnosti. Písemná forma je zachována i při právním jednání učiněném elektronickými nebo jinými technickými prostředky umožňujícími zachycení jeho obsahu a určení jednající osoby ve smyslu § 562 Občanského zákoníku. Při doručování prostřednictvím doporučeného psaní nastávají účinky doručení okamžikem přijetí doručované písemnosti adresátem od poštovního doručovatele dle platných poštovních podmínek uveřejněných



na základě zákona č. 29/2000 Sb., o poštovních službách, ve znění pozdějších předpisů. Doporučené psaní adresované Smluvní straně Smlouvy je třeba adresovat vždy na adresu Smluvní strany uvedenou ve Smlouvě. Tato doručovací adresa Smluvní strany může být změněna pouze písemným oznámením doručeným druhé Smluvní straně. Pro doručování jiných poštovních zásilek než písemností platí toto ustanovení této Smlouvy obdobně.

- 20.6. Smlouva obsahuje úplnou a jedinou písemnou dohodu Smluvních stran o vzájemných právech a povinnostech upravených Smlouvou.
- 20.7. Smlouva může být měněna pouze dohodou Smluvních stran v písemné formě prostřednictvím vzestupně číslovaných dodatků, přičemž změna Smlouvy bude účinná k okamžiku stanovenému v takovéto dohodě. Nebude-li takovýto okamžik stanoven, pak změna Smlouvy bude účinná ke dni uzavření takovéto dohody. Při uzavírání takové dohody budou respektovány veškeré limity vyplývající ze zákonné úpravy zadávání veřejných zakázek.
- 20.8. Smlouva je vyhotovena ve 4 stejnopisech, přičemž Objednatel obdrží 3 stejnopisy a Dodavatel 1 stejnopis.
- 20.9. Nedílnou součástí Smlouvy tvoří tyto přílohy:
- Příloha č. 1 – Projektový a investiční záměr SOCCR
 - Příloha č. 2 – Specifikace požadavků na Technický projekt
 - Příloha č. 3 – Harmonogram plnění
 - Příloha č. 4 – Stanovené ceny MD
 - Příloha č. 5 – Metodika projektového řízení
 - Příloha č. 6 – Vzor rozkladu dodávky na položky

V Praze dne 22.12.2014

Ministerstvo vnitra ČR
Mgr. Bohdan Urban,
ředitel odboru eGovernmentu

V Praze dne 22.12.2014

Česká pošta, s.p., Odštěpný závod ICT služby
Jan Přerovský,
vedoucí Odštěpného závodu ICT služby



HARDWARE

INFRASTRUKTURA

SOFTWARE

KOMUNIKACE

BEZPEČNOST

VEŘEJNÉ ZAKÁZKY



Projektový a investiční záměr

Dohledové centrum SOCCR

 **Česká pošta**
odštěpný závod **ICT služby**

Verze 1.4

Česká pošta, s.p., Odštěpný závod ICT služby, Kodaňská 46/1441, 101 00 Praha 10
+420 234 066 500, ID datové schránky: kr7cdry, IČ: 47114983

ID P001.02.01-01
Klasifikace Interní



Projektový a investiční záměr, verze 1.4

Ochrana informací

Informace obsažené v tomto dokumentu byly vypracovány organizací Česká pošta s.p., Odštěpný závod ICT Služby, Olšanská 4, Praha 3 v rámci projektu Dohledové centrum SOCCR a jako takové slouží výhradně k účelům tohoto projektu. Jsou určeny pouze pro Ministerstvo vnitra ČR a nemohou být poskytovány v jakékoli podobě dalším subjektům bez souhlasu výše uvedených organizací.



IDENTIFIKACE DOKUMENTU

1. Identifikace	P001.02.01-01
2. Klasifikace	Interní
3. Název	Projektový a investiční záměr
4. Projekt	Dohledové centrum SOCCR
7. Verze	Verze 1.3
9. Počet stran	27 stran
10. Verze šablony	Základní šablona pro MS Word platná ke dni 27/07/2014
12. Vytvořil	Roman Smetana, Michal Vodička, Jan Mikulecký

PREAMBULE

Tento dokument vytvořil pracovní tým Odštěpného závodu České pošty s.p. (dále též „ČPOZ“) v rámci prací na projektu „Dohledové centrum SOCCR“ pro Ministerstvo vnitra (dále též „MV“) v souladu se zadáním Komise pro kybernetickou bezpečnost Ministerstva vnitra ze dne 20/10/2014 a objednávkou MV-46080-22/EG-2014.

Záměr byl vytvořen pro podporu investice do Dohledového centra MV pro provoz ICT systémů a kybernetickou bezpečnost (dále jen SOCCR). Dohledové centrum rozšiřuje funkčnost servisní platformy eGovernmentu v rámci Centrálního místa služeb a naplňuje požadavky zákona 181/2014 o kybernetické bezpečnosti. Dohledové centrum SOCCR je navrženo plně v souladu se schválenou Strategií kybernetické bezpečnosti na roky 2012 – 2015, stejně tak s budoucí, zatím neschválenou, strategií na roky 2015 – 2020 (ve fázi přípravy).

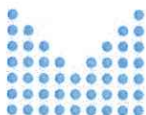
Zpracovatel dokumentu prohlašuje, že jsou mu známy veškeré dokumenty, podmínky a materiály týkající se projektů ITS NGN, KSP, NIS IZS a CMS ke dni zpracování Projektového záměru, že byly zohledněny v maximální možné míře pro tvorbu tohoto materiálu a zejména architektury SOCCR a že neočekává odchylky (při zachování znění výše uvedených projektů) od tohoto stavu v průběhu dodávky komponent SOCCR podle tohoto dokumentu. Dále zpracovatel prohlašuje, že mu nejsou známy žádné omezující podmínky neuvedené v tomto materiálu vyplývající zejména z projektů kofinancovaných v rámci IOP navazujících na SOCCR.“

PODĚKOVÁNÍ

Pracovní analytický tým by rád poděkoval dalším kolegům z odboru systémové integrace projektů a oddělení bezpečnosti za jejich spolupráci a pomoc při vytváření záměru a během přípravy tohoto dokumentu.

HISTORIE ZMĚN

1.0	14/11/2014	Základní dokument
1.1	14/11/2014	Formální úpravy
1.2	24/11/2014	Formální úpravy, vyřízení komentářů ze dne 19/11/2014
1.3	6/12/2014	Doplnění vazby na NCKB; provázání paragrafů zákona s technologiemi
1.4	17/12/2014	Upraven popis servisní platformy, doplněny přílohy



Projektový a investiční záměr, verze 1.4

SCHVÁLENÍ

Obsah tohoto dokumentu je schválen podpisy následujících:

Jméno	Organizace	Podpis	Funkce v projektu / organizaci	Datum	Verze
Jan Mikulecký	ČPOZ		Vedoucí projektu / Vedoucí bezpečnostního oddělení		1.4
Jan Přerovský	ČPOZ		Ředitel		1.4



OBSAH

Identifikace dokumentu	3
Preambule	3
Poděkování	3
Historie změn	3
Schválení	4
Obsah	5
1 Pozadí záměru dohledového centra	6
1.1 Zákon 181/2014 o kybernetické bezpečnosti	6
1.2 Analýza souladu systémů MV s požadavky zákona 181/2014	7
1.3 Dohledové centrum	7
1.4 Role vyplývající z kybernetického zákona	8
2 Návrh řešení CMS 2.0 a SOCCR	10
2.1 Opatření vyplývající z kybernetického zákona	10
2.2 Základní služby SOCCR	11
2.3 Řízení bezpečnosti v aktivním a pasivním módu	12
2.4 Technologické řešení a nástroje SOCCR	12
2.5 Rozšíření servisní platformy	14
2.6 Propojení SOCCR na NCKB (Národní centrum kybernetické bezpečnosti)	14
2.7 Propojení na další složky státu	15
3 Architektura řešení	16
3.1 Popis architektury z pohledu komunikačních vrstev	17
3.2 Integrace SOCCR a CMS 2.0	18
3.3 Popis architektury dohledového centra	22
3.4 Kapacitní požadavky SOCCR (rozšíření CMS)	23
3.5 Fáze integrace	23
3.6 Předpokládaný harmonogram	24
3.7 Certifikace ISMS	24
3.8 Umístění zařízení SOCCR	24
3.9 Rámcový rozpočet	25
4 Seznam zkratek	27



Projektový a investiční záměr, verze 1.4

1 POZADÍ ZÁMĚRU DOHLEDOVÉHO CENTRA

Oblast kybernetické bezpečnosti nabývá neustále na svém významu a již nyní platí za jeden z určujících aspektů bezpečnostního prostředí České republiky. Kybernetická bezpečnost představuje souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v České republice, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost. Kybernetická bezpečnost pomáhá identifikovat, hodnotit a řešit hrozby v kyberprostoru, snižovat kybernetická rizika a eliminovat dopady kybernetických útoků, informační kriminality, kyberterorismu a kybernetické špionáže ve smyslu posilování důvěrnosti, integrity a dostupnosti dat, systémů a dalších prvků informační a komunikační infrastruktury. Hlavním smyslem kybernetické bezpečnosti je pak ochrana prostředí k realizaci informačních práv člověka.

Strategie kybernetické bezpečnosti resortu vnitra vychází z Národní strategie kybernetické bezpečnosti České republiky, jejího legislativního rámce, zejména zákona o kybernetické bezpečnosti, zákona o krizovém řízení a s tím souvisejících prováděcích vyhlášek a norem ČSN a doporučení ISO/IEC, zejména rodiny norem 27k.

Taktéž potřeba zajistit jednotnou platformu dohledu pro vznikající projekty MV je důvodem k realizaci projektu jako celku.

1.1 ZÁKON 181/2014 O KYBERNETICKÉ BEZPEČNOSTI

Prezident republiky Miloš Zeman podepsal dne 13. srpna 2014 zákon č. 181/2014 o kybernetické bezpečnosti (ZoKB). Zákon bude účinný od 1. ledna 2015 a určuje pro osoby povinné přechodné období do 1. ledna 2016.

OSOBY POVINNÉ

Rozsah dopadu zákona na Ministerstvo vnitra vyplývá z §3, který definuje osoby povinné:

Orgány a osobami, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti, jsou:

- a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací¹⁾, pokud není orgánem nebo osobou podle písmene b),*
- b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem komunikačního systému podle písmene d),*
- c) správce informačního systému kritické informační infrastruktury,*
- d) správce komunikačního systému kritické informační infrastruktury a*
- e) správce významného informačního systému.*

Prováděcí předpisy, které určují kritické a významné informační systémy jsou k datu zpracování tohoto dokumentu (listopad 2014) v meziresortním připomínkovém řízení. Z předběžných předpokladů lze však odvodit, že řada systémů resortu MV bude určena jako kritické nebo významné.

NAŘÍZENÍ VLÁDY O KRITÉRIÍCH PRO URČENÍ PRVKU KRITICKÉ INFRASTRUKTURY Č. 432/2010

Předpis definuje průřezová a odvětvová kritéria, podle nichž se určují prvky kritické infrastruktury a informační nebo komunikační systémy kritické infrastruktury.

VYHLÁŠKA O URČENÍ VÝZNAMNÝCH SYSTÉMŮ

Významné systémy jsou určeny podle dopadových a oblastních kritérií. Aby byl systém označen za významný, musí splňovat minimálně jedno z obou kategorií kritérií. V případě, že systém byl již



označen jako informační nebo komunikační systém kritické infrastruktury dle nařízení vlády 432/2010, je splnění kritérií pro významné systémy pouze doplňující a informativní.

VYHLÁŠKA O BEZPEČNOSTNÍCH OPATŘENÍCH

Národní bezpečnostní úřad vypracoval návrh vyhlášky o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) k provedení zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Tato vyhláška přesně určuje, která opatření ve formě technologií, procesů a lidských zdrojů musí být zavedena pro zajištění kybernetické bezpečnosti. Tento etalon byl základním vstupem pro stanovení funkčních požadavků, které musí dohledové centrum SOCCR splňovat.

DALŠÍ ZÁKONNÉ ÚPRAVY

Oblast kybernetické bezpečnosti má oporu také v další legislativě, která byla vstupem pro zpracování tohoto záměru. Primárně se jedná o zákon č. 127/2005 Sb., o elektronických komunikacích a zákon č. 240/2000 Sb., o krizovém řízení.

1.2 ANALÝZA SOULADU SYSTÉMŮ MV S POŽADAVKY ZÁKONA 181/2014

K 30/11/2014 byla dokončena analýza systémů MV z pohledu naplnění požadavků kybernetického zákona. V rozsahu analýzy bylo 52 systémů spravovaných odbory MV, HZS, PČR a SZR. V rámci analýzy bylo určeno 24 systémů, které byly klasifikovány jako kritické nebo významné. Každý z těchto systémů bude dohlížen v rámci centra SOCCR a řada technických opatření kybernetické bezpečnosti bude zajištěna v rámci projektu SOCCR.

I přesto, že detailní bezpečnostní nedostatky v daných systémech ukáže až dokončená analýza, již nyní lze predikovat určitou úroveň nesouladu s novým zákonem. Systémy MV bude nutné doplnit o bezpečnostní technologie a také zajistit odpovídající úroveň provozního dohledu. Jeho současný stav představuje finanční a provozní rizika, která mohou významně ovlivnit dostupnost informačních systémů resortu MV.

Neexistuje zde jednotná koncepce, jednotlivé oblasti jsou řešeny proprietárně a ad-hoc. Využité produkty nepodporují současné technologie a v používaných verzích nejsou možná rozšíření. Pro dohled a servisní platformu jsou využívány zastaralé produkty, některé již za hranou životnosti a pro zajištění provozu by bylo nutné zakoupení aktuálních produktů, jejich licencí a migrace na nové produkty. Není též zajištěna jednotná strategie pro jednotlivé servisní platformy, což má za následek nedostupnost klíčových informací i v době incidentu vedoucí k prodloužení doby obnovy služeb.

1.3 DOHLEDOVÉ CENTRUM

Záměr vybudovat Dohledové centrum MV pro provoz ICT systémů a kybernetickou bezpečnost (dále jen SOCCR) pokrývá výše uvedené nedostatky a zároveň nové požadavky na zajištění souladu s novou legislativou. Projekt provozního a bezpečnostního dohledového centra SOCCR je navržen s cílem naplnit většinu technologických požadavků kybernetického zákona a souvisejících vyhlášek. Pro zajištění řádného řízení bezpečnosti jsou navrženy i další technologie nevyžadované přímo kybernetickým zákonem. Cílem je zajistit komplexní řízení bezpečnosti systémů MV, a proto jsou nad rámec legislativních požadavků navrženy další technologická opatření a bezpečnostní nástroje.

Zároveň bude zajištěn rozvoj portálu servisní platformy, Service Desk, provozní monitoring, provisioning, billing a reporting. Rozvoj financovaný v rámci tohoto záměru spočívá ve vytvoření



Projektový a investiční záměr, verze 1.4

funkčního celku bezpečnostního dohledového centra, včetně zajištění provozního dohledu ITS/CMS a umožní rozšířit provozní dohled pro projekty NIS ISZ a KSP v rozsahu definovaném v kap. 2.5.

Dohledové centrum rozšiřující funkčnost CMS 2.0 je navrženo tak, aby se stalo jeho integrální součástí. Tento záměr byl připravován týmem architektů a bezpečnostních specialistů, kteří jsou zároveň členy projektového týmu, jež dodává projekt CMS 2.0 na základě Smlouvy o dílo č.j. MV-42584-210/KAP-2009 ze dne 10.1.2014. Výstupy byly také průběžně konzultovány s hlavním architektem eGovernmentu (Ondřej Felix). Tímto je v maximální míře zajištěno, že nedojde například k duplikaci systémů či absenci tolik požadované provázanosti a to v žádné fázi projektu.

V případě požadavku se strany MV lze do dohledového centra zapojit i standardní systémy nepodléhající kybernetickému zákonu. Provozní i bezpečnostní dohled je vhodné řešit i na standardních systémech, které nejsou přímo regulovány novou legislativou.

Součástí tohoto záměru je vytvoření platformy (technologií a procesů), která může být následně aplikována i nad aktuálně zamýšlený rozsah, včetně systémů mimo resort MV. Architektura dohledového centra SOCCR je navržena variabilně se snadnou možností dalšího rozvoje. Lze předpokládat, že SOCCR může v dalších letech dohledovat i jiné systémy, na které se zákon o kybernetické bezpečnosti nevztahuje.

Řádné řízení bezpečnosti, které lze prostřednictvím SOCCR prosadit i na další systémy, je obecným cílem pro všechny informační a komunikační prvky nejen resortu Ministerstva vnitra. I přesto, že napojení dalších systémů do dohledového centra přinese na jejich straně určité finanční nároky, za všech okolností bude **nákladově efektivní sdružit bezpečnostní technologie a zajistit jednotné řízení kybernetické bezpečnosti skrze SOCCR.**

1.4 ROLE VYPLÝVAJÍCÍ Z KYBERNETICKÉHO ZÁKONA

Zákon 181/2014 o kybernetické bezpečnosti předepisuje také zajištění organizační bezpečnosti. Vyhláška o bezpečnostních opatřeních (zatím nevydaná) stanoví jednotlivé role a jejich odpovědnosti pro oblast kybernetické bezpečnosti. V souladu s těmito požadavky musí být obsazeny role níže uvedené role v kontextu poskytovaných služeb centrem SOCCR i pro vybrané systémy zařazené do kategorie „kritický“ nebo „významný“.

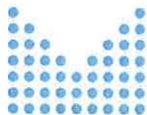
Manažer kybernetické bezpečnosti je osoba odpovědná za systém řízení bezpečnosti informací, která je pro tuto činnost řádně vyškolená a prokáže odbornou způsobilost praxí s řízením bezpečnosti informací po dobu nejméně tří let. Role bude obsazena pracovníkem MV.

Architekt kybernetické bezpečnosti je osoba odpovědná za návrh a implementaci bezpečnostních opatření, která je pro tuto činnost řádně vyškolená a prokáže odbornou způsobilost praxí s navrhováním bezpečnostní architektury po dobu nejméně tří let. Role bude obsazena pracovníkem odboru hlavního architekta MV.

Auditor kybernetické bezpečnosti je osoba odpovědná za provádění auditu kybernetické bezpečnosti, která je pro tuto činnost řádně vyškolená a prokáže odbornou způsobilost praxí s prováděním auditů kybernetické bezpečnosti po dobu nejméně tří let (např. auditor ISMS). Role bude obsazena pracovníkem odboru interního auditu MV.

Garant aktiva fyzická osoba pověřená k zajištění rozvoje, použití a bezpečnosti aktiva, kterým se rozumí prvek informačního systému, např. hardware, software, data atd. Tato bude obsazena pracovníkem MV.

Školení a zvyšování bezpečnostního povědomí - v rámci řešení je počítáno i s dalším požadavkem zákona, který úzce souvisí s organizační bezpečností, týkající se zavedení vzdělávání, pravidelného školení a zvyšování povědomí v oblasti bezpečnosti. Budoucí kompetenční centrum bezpečnosti ČP



OZ je připraveno poskytovat proškolení všech pracovníků z oblasti kybernetické bezpečnosti na různých úrovních a zaměření.



Projektový a investiční záměr, verze 1.4

2 NÁVRH ŘEŠENÍ CMS 2.0 A SOCCR

Základní myšlenkou technologické integrace SOCCR a CMS 2.0 je předpoklad, že informační ochranu nelze zajistit pouze z pohledu projektu. Bezpečnost informací je v jednotlivých systémech řešená individuálně s omezením se na jejich rozsah a nejde za jejich hranice. Prostředí, ve kterém systémy fungují je širší a představuje celou informační infrastrukturu veřejné správy. Například nelze řídit bezpečnost odděleně nad různými prostředími, která jsou tvořena nebo rozvíjena v rámci rozdílných projektů, které spolu komunikují, a není mezi nimi jasně stanovená hranice.

Takto je třeba chápat i prostředky ochrany takového prostředí. Komunikační prostředí jednotlivých státních institucí je nejen propojené vzájemně, ale i s dalšími institucemi v České republice i evropskými orgány. Na tomto základě vznikla potřeba integrovat informační bezpečnost jako liniový projekt, který zajišťuje právě tento přesah. Stejně tak nově vydaný zákon o kybernetické bezpečnosti chápe zajištění bezpečnosti v kontextu státním i celosvětovém.

Návrh dohledového centra SOCCR vychází z plánovaného stavu Centrálního místa služeb (projekt CMS 2.0), jehož znalost je nutná k řádnému pochopení dále navrhovaného řešení. V souladu se záměrem hlavního architekta eGov se SOCCR stane integrální součástí CMS a bude připraven dohlížet kritické a významné systémy MV.

2.1 OPATŘENÍ VYPLÝVAJÍCÍ Z KYBERNETICKÉHO ZÁKONA

Níže je uveden výčet vybraných řešení, které spolu s procesy, dokumentací a konfigurací tvoří systém pokrývající povinnosti vyplývající z jednotlivých paragrafů vyhlášky o bezpečnostních opatřeních k zákonu č. 181/2014 o kybernetické bezpečnosti a jeho výkladu:

1. Nástroj pro řízení rizik – § 3., §4., § 28., §29.
2. Nástroj pro havarijní plánování a zajištění obnovy služeb - § 3.
3. Nástroje autentizační podpory pro privilegované operace - § 11., § 18., § 19.
4. SIEM pro centrální správu a řízení bezpečnosti - §10., §13., §21., §23.
5. Nástroj pro řízení technických zranitelností všech komunikačních bodů - § 15., §27.
6. Antivirové řešení a nástroj pro ochranu před malware - § 20.
7. Nástroj pro detekci kybernetických bezpečnostních událostí - § 22.
8. Řízení přístupu do sítě - § 17.

V případě MV se jedná o rozšíření provozního dohledu CMS 2.0 a bezpečnostního dohledu tak, aby pokrýval i oblasti mimo rozsah projektu CMS 2.0 a to na různých logických i komunikačních vrstvách. Je známá situace, kdy se bezpečnostní opatření jednotlivých projektů překrývají a zdvojují, v jiných případech naopak nedoléhají a vznikají nepokryté oblasti. Smyslem integrace a rozšířením oblasti pokrytí bezpečnosti je tedy ušetřit finanční prostředky, sjednotit přístup pro řízení bezpečnosti a zároveň ji povýšit ošetřením všech potenciálních hrozeb. Koncept bezpečnostního dohledu SOCCR si spolu s rozšířením CMS 2.0 o větší provozní dohled klade právě tyto cíle.

2.2 ZÁKLADNÍ SLUŽBY SOCCR

Dohledové centrum SOCCR poskytuje služby pro řízení bezpečnosti v připojených systémech. Zároveň naplňuje technické požadavky kybernetického zákona a související legislativy, mezi které patří dohledování systémů, skenování zranitelností, řízení privilegovaných přístupů apod.



Obrázek 1 – Základní služby SOCCR

Služby, které SOCCR poskytuje, jsou uvedeny níže. Detaily k pasivnímu a aktivnímu módu a z toho vyplývajících služeb jsou uvedeny v následující kapitole.

- Sbírá a vyhodnocuje provozní a bezpečnostní události v režimu 24x7
- Identifikuje a řeší bezpečnostní incidenty
- Hlásí incidenty do NCKB
- Naplňuje technické požadavky kybernetického zákona
- Řídí bezpečnost v aktivním a pasivním módu
- Automatizovaně skenuje zranitelnosti
- Poskytuje bezpečnostní reporting
- Zajišťuje certifikační autoritu
- Zajišťuje DDoS ochranu (prostřednictvím CMS)
- Podporuje procesy řízení rizik a kontinuity
- Tým SOCCR = Cyber Incidents Response Team
- Zajišťuje informační fórum pro bezpečnostní správce a manažery
- Zajišťuje služby forenzní laboratoře, skenuje externí prostředí, fóra, sociální sítě (vize 2016+)

V rámci Centrálního místa služeb jsou zajištěny následující služby, které souvisí s dohledovým centrem SOCCR, více viz kapitola 2.5 Rozšíření servisní platformy.

- Provozní monitoring
- Billing
- Provisioning
- Service Desk
- LDAP/IAM
- eGSB
- Log Management
- SysLog Server



2.3 ŘÍZENÍ BEZPEČNOSTI V AKTIVNÍM A PASIVNÍM MÓDU

Jednotlivé systémy mohou být připojeny v různých módech od kompletního řízení bezpečnosti až po pasivní dohlížení části systému. V aktivním módu přebírá SOCCR odpovědnost za zajištění kybernetické bezpečnosti informačního systému a naplnění technických požadavků kybernetického zákona. Pasivní mód je vhodný pro systémy, kde existují kvalitní procesy řízení bezpečnosti a je potřebné jen doplnit chybějící bezpečnostní dohled, skenování technických zranitelností, případně dílčí procesy v oblasti řízení rizik a kontinuity činnosti. Detailní specifikace módů, včetně definice rozhraní na systémy bude předmětem technického projektu SOCCR (1Q 2015). Dohledové centrum bude připraveno na kombinaci obou módů a přizpůsobení vybraných parametrů podle požadavků jednotlivých systémů.

Aktivní mód – řídí bezpečnost	Pasivní mód – dohlíží bezpečnost
SOCCR je bezpečnostní administrátor systému	SOCCR je dohlížitel - pouze dostává informace ze systému
SOCCR analyzuje, vyhodnocuje a dává informace zpět do systému, <u>aktivně řeší incident</u> (technicky, procesně), ve spolupráci s administrátory zasahuje do konfigurace	SOCCR analyzuje, vyhodnocuje a dává informace zpět do systému, <u>dává doporučení na reakci</u>
SIEM – v systému je implementována sonda/agent, sbírá události, vyhodnocuje, do SOCCR zasílá agregované údaje	SIEM – získává agregované události z koncového systému pomocí systémového účtu, logy se analyzují až v SOCCR
SOCCR vyžaduje plný přístup do systému, implementaci nástroje PIM/PAM + 2FA (administrátorské přístupy)	N/A – SOCCR má pouze přístup „pro čtení“
SOCCR provádí automatizované skenování zranitelností s autentizací	SOCCR (ne-)pravidelně skenuje zranitelnosti bez autentizace (s povolením správce systému)
HoneyPot – implementován v (interní) síti, aktivně dohleduje technologií IPS/IDS	N/A
Podpora procesů řízení rizik a kontinuity (SOCCR má nástroj)	SOCCR neřeší procesy RM a BCM, pouze jednoduchá metodická podpora zdarma

Tabulka 1: Aktivní a pasivní mód SOCCR

2.4 TECHNOLOGICKÉ ŘEŠENÍ A NÁSTROJE SOCCR

V souvislosti s uvedeným záměrem a požadavky zákona o kybernetické bezpečnosti budou implementovány následující bezpečnostní opatření, technologie a procesy, vyplývající z výše uvedených paragrafů, které budou vzájemně i návazně integrovány s CMS. Součástí dohledového centra SOCCR jsou i další technologie (např. HoneyPot), jejichž implementace není explicitně vyžadována zákonem 181/2014 nebo souvisejících vyhlášek. Cílem projektu SOCCR je zajistit řádné komplexní řízení bezpečnosti systémů MV, a proto jsou navrženy také technologie a nástroje, které jsou nad rámec legislativních požadavků.

Jádrem dohledového centra je systém SIEM (Security Information & Event Management), který shromažďuje logy a záznamy z připojených systémů. Využití SIEM vyplývá z požadavků zákona uvedených v §10., §13., §21., §23. Analyzuje informace s cílem identifikovat potenciální bezpečnostní incidenty. Jeho součástí jsou také nástroje pro forenzní analýzy. Systém SIEM je budován v rámci projektu CMS 2.0 a bude v rámci dalšího rozvoje SOCCR rozšířen tak, aby bylo možné pokrýt i další systémy resortu MV. SIEM je financován v rámci projektu CMS 2.0.

Součástí dohledového centra je systém IPS/IDS – Intrusion prevention/detection system pro zajišťování bezpečnosti síťového provozu vyplývající z § 22 a § 17 kybernetického zákona. Jeho



prostřednictvím lze detekovat, vyhodnocovat a blokovat pokusy o průnik na síťové vrstvě a anomálie datového provozu. Systém je integrován se SIEM a předává své stavy a události pro další korelaci. Systém IPS/IDS je budován v rámci projektu CMS 2.0 a bude v rámci dalšího rozvoje SOCCR rozšířen tak, aby bylo možné pokrýt i další systémy resortu MV. Systém IDS/IPS je financován v rámci projektu CMS 2.0.

V rámci projektu CMS 2.0 je implementováno řešení pro automatizované, periodické a nepřetržité **testování technických zranitelností**, které pokrývá požadavky § 15., §27. Toto řešení, které je financováno v rámci projektu CMS 2.0, bude integrováno do dohledového centra SOCCR a spojeno se SIEM.

Ochrana proti virům je běžným požadavkem ve všech systémech, a proto je zde navržena implementace dvouvrstvého antivirového řešení, které slouží k identifikaci, odstraňování a eliminaci počítačových virů a jiného škodlivého softwaru. Požadavek na implementaci tohoto systému vyplývá z § 20 zákona. Systém antivirus bude implementován jednak pro perimetr CMS 2.0 a také pro samotné centrum SOCCR. Dohledované systémy, které mají vlastní antivirové řešení, budou pro SOCCR, resp. pro SIEM, poskytovat provozní a bezpečnostní události. Toto řešení, je financováno částečně v rámci projektu CMS 2.0 - vnější perimetr a částečně ze zdrojů dohledového centra SOCCR – vnitřní perimetr.

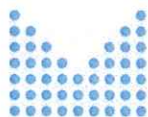
Provozování kritické infrastruktury a systémů významných pro chod státu vyžaduje striktní řízení přístupů odpovědných administrátorů a správců. Privilegované činnosti v informačních systémech jsou velmi citlivou oblastí a administrátoři mohou i neúmyslně způsobit značný negativní dopad při nesprávném nastavení parametrů nebo jiných činnostech správy ICT. V rámci SOCCR je zavedeno striktní **řízení privilegovaných přístupů**, které zajistí ochranu silných administrátorských hesel, jejich efektivní využívání a automatickou obměnu v připojených systémech. Použití tohoto nástroje pokrývá požadavky § 11., § 18., § 19 zákona. Zároveň jsou všechny privilegované činnosti detailně logovány. Toto řešení je financováno z rozpočtu dohledového centra SOCCR, viz kap. 3.9.

Součástí řešení pro privilegované přístupy je **dvoufaktorová autentizace** pro ochranu identity administrátorů jednotlivých systémů. Tento způsob autentizace bude využitý pro privilegované (administrátorské) přístupy dohledovaných systémů. Toto řešení je financováno z rozpočtu dohledového centra SOCCR, viz kap. 3.9.

Informace o rizicích budou mít vazbu na další hodnotící systémy, např. řešení pro hodnocení technických zranitelností a provádění auditů konfigurace (viz výše). **Nástroj pro řízení rizik**, kterým budou naplněny paragrafy § 3., §4., § 28., §29, umožní nastavit systematický a metodický přístup k identifikaci a hodnocení informačních rizik. Cílem implementace je jasný a komplexní pohled na rizika, která jsou provázána na všechna aktiva zahrnutých informačních systémů. Toto řešení je financováno z rozpočtu dohledového centra SOCCR, viz kap. 3.9.

Procesy **řízení kontinuity** a obnovy po havárii zde budou řízeny pomocí nástroje pro řízení kontinuity činností (BCM), který úzce souvisí s výše uvedeným nástrojem pro řízení rizik a může jím být naplněn § 3 zákona. Základním předpokladem začlenění je možnost tvorby a údržby dokumentů souvisejících s BCM. Nástroj zpřístupní administrátorům dohledovaných systémů relevantní plány kontinuity a obnovy a další potřebné informace podporující řešení krizových situací. Součástí projektu SOCCR je vytvoření plánů kontinuity a obnovy pro samotné dohledové centrum. Dokumentace BCM pro dohledované systémy nebude financována v rámci projektu SOCCR, nicméně bude k dispozici výše uvedený nástroj pro BCM. Toto řešení je financováno z rozpočtu dohledového centra SOCCR, viz kap. 3.9.

V dohledovém centru SOCCR bude k dispozici HoneyPot, který v případě implementace do SOCCR představuje doplněk k systémům IDS/IPS a Netflow. HoneyPot bude řešen rozmístěním strojů/systémů na virtualizační platformě s aplikační částí, která emuluje chod standardních



Projektový a investiční záměr, verze 1.4

systémů nebo sítí. Komunikace směřovaná na tyto zdroje je následně vyhodnocována ze dvou vektorů. Vnější vektor představuje identifikaci komunikace vnějšími systémy a slouží k včasnému odhalení neoprávněné komunikace. Vnitřní vektor zachytává danou komunikaci pro následnou analýzu a umožňuje doplnit celkový obraz aktuální bezpečnostní situace vzhledem ke komunikaci. Toto řešení je financováno z rozpočtu dohledového centra SOCCR, viz kap. 3.9.

2.5 ROZŠÍŘENÍ SERVISNÍ PLATFORMY

Portál servisní platformy, který je součástí projektu CMS 2.0, zajišťuje Service Desk, provozní monitoring, provisioning, billing a reporting pro Centrální místo služeb není součástí tohoto projektového záměru. V rámci projektu SOCCR je zajištěno (a financováno) rozšíření licencí pro výše uvedené služby systémů NIS ISZ, KSP a ITS NGN dle zadání těchto projektů a to dle rozpočtu v kap. 3.9. ve výši 5.945tis. Pro plné fungování servisní platformy je nutné rozšířit projekt v dalších etapách o celkové požadavky všech uvedených projektů. Tyto technické specifikace projektů budou zpracovány v technickém projektu, který bude výstupem první fáze. Součástí bude harmonogram a cenové ohraničení dalších fází.

Technologické řešení, které je finančně zajištěno z projektu CMS 2.0 bude možné licenčně rozšířit o možnost poskytovat své služby i pro systémy NIS ISZ, KSP a ITS NGN

Plné rozšíření servisní platformy o celkové nároky všech výše uvedených projektů, včetně call centra, jeho vybavení a personálního obsazení není finančně zajištěno v rámci rozpočtu uvedeném v kap. 3.9. Toto rozšíření bude specifikováno v rámci Technického projektu jako rozšíření projektového záměru SOCCRu.

Dohledové centrum bude připraveno, aby pro významné a kritické systémy MV zajišťovalo v rámci servisní platformy také následující služby:

- Portál servisní platformy jako centrální bod přístupu uživatelů
- Service desk jako centrální řídicí bod pro veškeré procesy
- Monitoring jako centrální bod pro sběr veškerých událostí a metrik z jednotlivých systémů
- Provisioning jako nástroj pro správu konfigurací jednotlivých komponent a služeb
- Billing jako nástroj pro sběr údajů potřebných k vyúčtování poskytovaných služeb
- Reporting pro jednotné řízení reportů celé platformy

Zajištění výše uvedených služeb pro významné a kritické systémy MV (vyjma ITS, NIS IZS a KSP) není součástí rozpočtu, který vychází z tohoto záměru dohledového centra SOCCR. Financování služeb servisní platformy pro jiné systémy MV, musí být řešeno individuálně. Bezpečnostní monitoring a další služby pro řádné řízení kybernetické bezpečnosti bude v rámci tohoto záměru pro kritické a významné systémy MV zajištěn.

2.6 PROPOJENÍ SOCCR NA NCKB (NÁRODNÍ CENTRUM KYBERNETICKÉ BEZPEČNOSTI)

Zákon o kybernetické bezpečnosti určuje v § 9 osobě povinné hlásit kybernetické bezpečnostní incidenty do Národního centra kybernetické bezpečnosti (NCKB). Požadavek musí být naplněn 1 rok od určení systémů jako kritického nebo významného a ne dříve než 1/1/2016.

Vyhláška o bezpečnostních opatřeních stanovuje typy a kategorie kybernetických bezpečnostních incidentů a náležitosti a formu jejich hlášení do NCKB. Incidenty je možné hlásit elektronickou, případně listinnou formou. Preferované jsou následující typy elektronické formy hlášení:

1. Prostřednictvím elektronického formuláře, který zatím není zveřejněn na internetových stránkách NBÚ ani NCKB



2. Zasláním emailu na adresu *cert.incident@nbu.cz*
3. Zasláním zprávy do datové schránky NBÚ *h93aayw*
4. Prostřednictvím datového rozhraní, jehož popis zatím nebyl ze strany NBÚ ani NCKB zveřejněn.

Lze předpokládat, že struktura hlášení incidentů bude odpovídat formuláři, uvedeném jako příloha č. 5 vyhlášky o kybernetických opatřeních. Formulář obsahuje obvyklé informace o bezpečnostních incidentech: identifikaci povinné osoby dle zákona, typ incidentu, jeho charakteristika, dopad, čas, místo, zasažený systém, opatření apod.

I přesto, že zatím nebyly zveřejněny detailní popisy všechny možností pro hlášení incidentů, bude v rámci dohledového centra SOCCR preferováno přímé napojení na datové rozhraní NCKB, aby hlášení o potenciálních incidentech bylo maximálně efektivní. Detailní popis procesu hlášení kybernetických incidentů a související technologická podpora bude součástí technického projektu SOCCR (1Q 2015), pokud budou v té době k dispozici detailní informace o datovém rozhraní. Návrh architektury propojení SOCCR na NCKB je uveden v kapitole 3.2.2, detailně viz Obrázek 4 – Integrace SIEM.

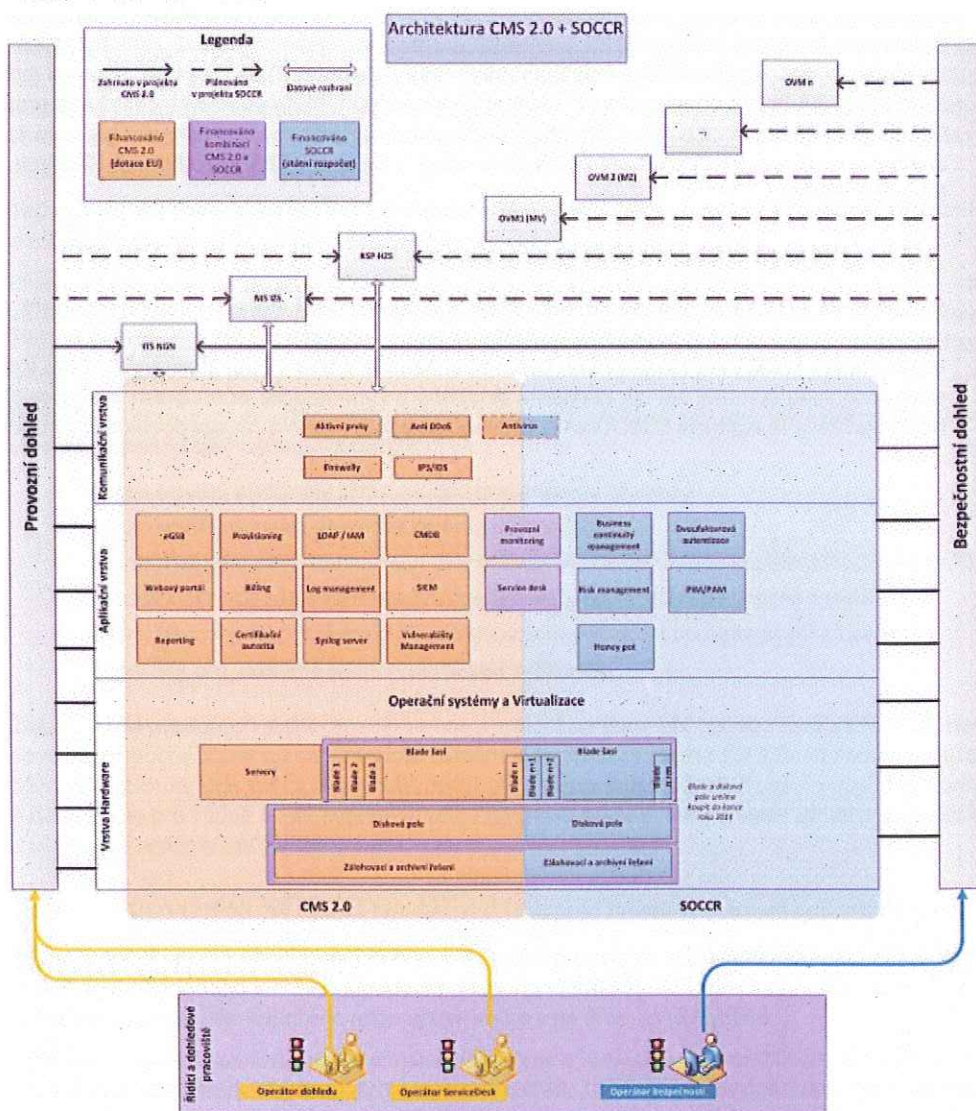
2.7 PROPOJENÍ NA DALŠÍ SLOŽKY STÁTU

SOCCR bude přímo napojen do Národního centra kybernetické bezpečnosti v Brně, které tvoří základní interface pro kybernetickou bezpečnost mezi jednotlivými složkami státu a komerčními organizacemi. SOCCR bude napojen na policejní systémy a systémy HZS, které byly určeny v rámci analýzy souladu systémů MV se zákonem 181/2014 o kybernetické bezpečnosti (listopad 2014). Nepředpokládá se napojení SOCCR na armádní systémy, které vyžívají vlastní dohledová centra.

Projektový a investiční záměr, verze 1.4

3 ARCHITEKTURA ŘEŠENÍ

Pro potřeby integrace SOCCR a CMS 2.0 byl navržen architektonický model, který popisuje logické propojení obou projektů, viz obrázek „Architektura CMS 2.0 + SOCCR“ a popis níže. Architektura celkového řešení je navržena tak, aby byly naplněny požadavky kybernetického zákona (modrá barva) pro systémy, které využívají nebo budou využívat CMS 2.0 a zároveň pro další systémy MV, které budou zákonu 181/2014 podléhat. Navržená architektura umožňuje rozšiřitelnost a škálovatelnost tak, aby mohly být uspokojeny potřeby i jiných (budoucích) systémů MV, případně i systémů ostatních resortů.



Obrázek 2 – Architektura CMS 2.0 + SOCCR



Jak ukazuje obrázek, bude realizován provozní i bezpečnostní dohled pro ITS NGN (integrovaná telekomunikační síť MV). Pro systémy NIS IZS a KSP budou provozní dohledy realizovány a financovány jsou součástí tohoto záměru SOCCR v rozsahu dle kap. 2.5. Pro významné a kritické systémy MV (v případě potřeby i pro standardní systémy) bude v rámci SOCCR řešen primárně bezpečnostní dohled. Provozní události budou zpracovávány v SIEM, nicméně řešení provozních dohledů významných a kritických systémů MV, vyjma výše vyjmenovaných, je záležitostí jednotlivých systémů.

3.1 POPIS ARCHITEKTURY Z POHLEDU KOMUNIKAČNÍCH VRSTEV

3.1.1 VRSTVA HARDWARE

HW vrstva spojuje vhodným způsobem virtualizační platformu s ohledem na výkon celého řešení tak, aby rozložení zátěže přes farmu blade serverů a zajištění dostupnosti bylo optimální. Tím je ošetřeno provozně neekonomické rozložení aplikací a využití serverů, např. situace, kdy v jednom šasi běží odděleně jen tři blade servery a tudíž není efektivně možné rozprostřít data nad více servery tak, aby byl při výpadku zachován provoz všech aplikací a s požadovanou odezvou. Předpokládá se tedy ideální sestavení zdrojů virtualizační platformy z obou zdrojů. Provoz operačních systémů nad touto vrstvou je pak řešen samostatně pro potřeby obou projektů. Předpokládá se, že alokace zdrojů pro provoz těchto OS bude v souladu investičním poměrem.

3.1.2 APLIKAČNÍ VRSTVA

Aplikační vrstva ve finální podobě integruje pouze prvky, které jsou pro oba celky společné. Kapacitně u nich dojde k navýšení prostředků ze zdrojů SOCCR tak, aby jednotlivé technologie byly schopné pokrýt potřebnou úroveň a rozsah dohledu v obou definovaných oblastech. Obrázek 1. obsahuje základní komponenty CMS 2.0 včetně provozního dohledu:

- Portál servisní platformy jako centrální bod přístupu uživatelů
- Service desk jako centrální řídicí bod pro veškeré procesy
- Monitoring jako centrální bod pro sběr veškerých událostí a metrik z jednotlivých systémů
- Provisioning jako nástroj pro správu konfigurací jednotlivých komponent a služeb
- Billing jako nástroj pro sběr údajů potřebných k vyúčtování poskytovaných služeb
- Reporting pro jednotné řízení reportů celé platformy

a dále komponenty bezpečnostního dohledu:

- SIEM pro centrální správu a řízení bezpečnosti
- Nástroj pro řízení technických zranitelností všech komunikačních bodů
- Nástroj pro jednotné řízení rizik
- Nástroj pro havarijní plánování a zajištění obnovy služeb
- Nástroje autentizační podpory pro privilegované operace
- Další nástroje ochrany dat a doplňkové bezpečnostní technologie

3.1.3 KOMUNIKAČNÍ VRSTVA

Komunikační vrstva nevyžaduje pro začlenění SOCCR do CMS 2.0 provedení změn. CMS 2.0 má robustní a dostatečně výkonově dimenzovanou infrastrukturu i pro nároky vyžadované ze strany SOCCR. Lze předpokládat, že všechna dohledovaná prostředí komunikují přes Centrální místo služeb nebo mohou být do tohoto uzlu připojena.

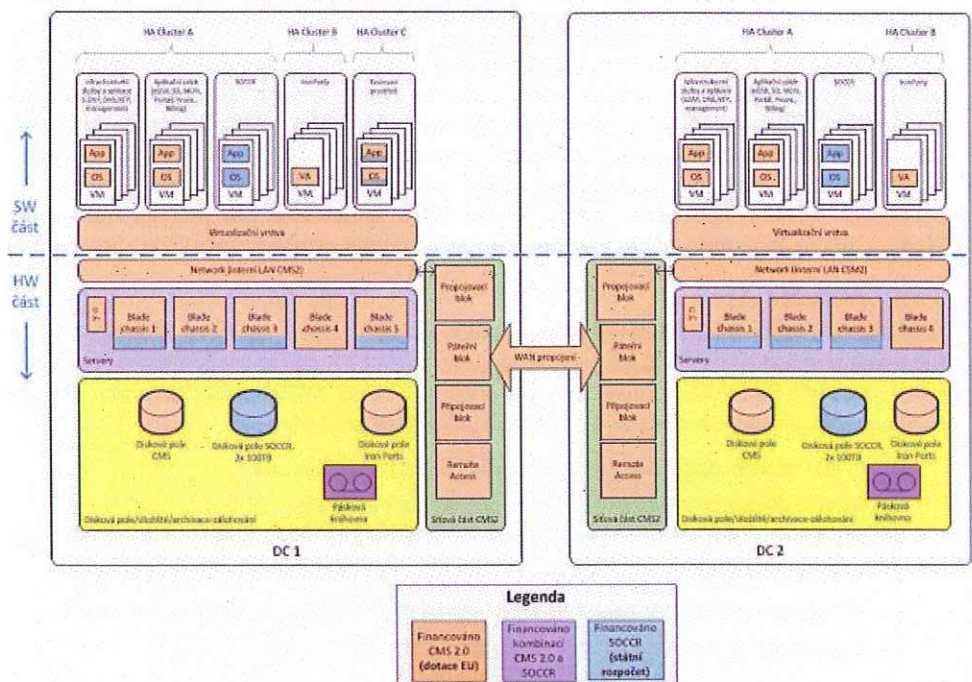
Projektový a investiční záměr, verze 1.4

3.2 INTEGRACE SOCCR A CMS 2.0

Integrace v zásadě představuje navrzení a propojení bezpečnostní infrastruktury a zároveň rozšíření stávající (navržené) bezpečnostní infrastruktury tak, aby v jednotlivých oblastech vytvářela homogenní systémy s ucelenou vnitřní koncepcí. Propojení je realizováno na více úrovních a je prováděno logicky i procesně tak, aby poskytovalo potřebnou ochranu z hlediska bezpečnosti. Pro přehlednost je popis rozdělen do více schémat.

3.2.1 INTEGRACE INFRASTRUKTURY

Na infrastrukturní vrstvě dochází k integraci zdrojů z obou částí projektů do homogenní platformy, která poskytne všem komponentám odpovídající požadované systémové zdroje.



Obrázek 3 – Integrace infrastruktury CMS 2.0 + SOCCR

V rámci virtualizační vrstvy jsou jednotlivé skupiny aplikací sloučeny do tzv. poolů, které umožní specifikovat požadavky na zdroje (výpočetní kapacity, rezervace zdrojů atp.). Tyto celky pak budou provozovány v HA clusterech, které zajistí vysokou dostupnost aplikací a dynamické rozdělování zátěže a kapacit v rámci jedné lokality.

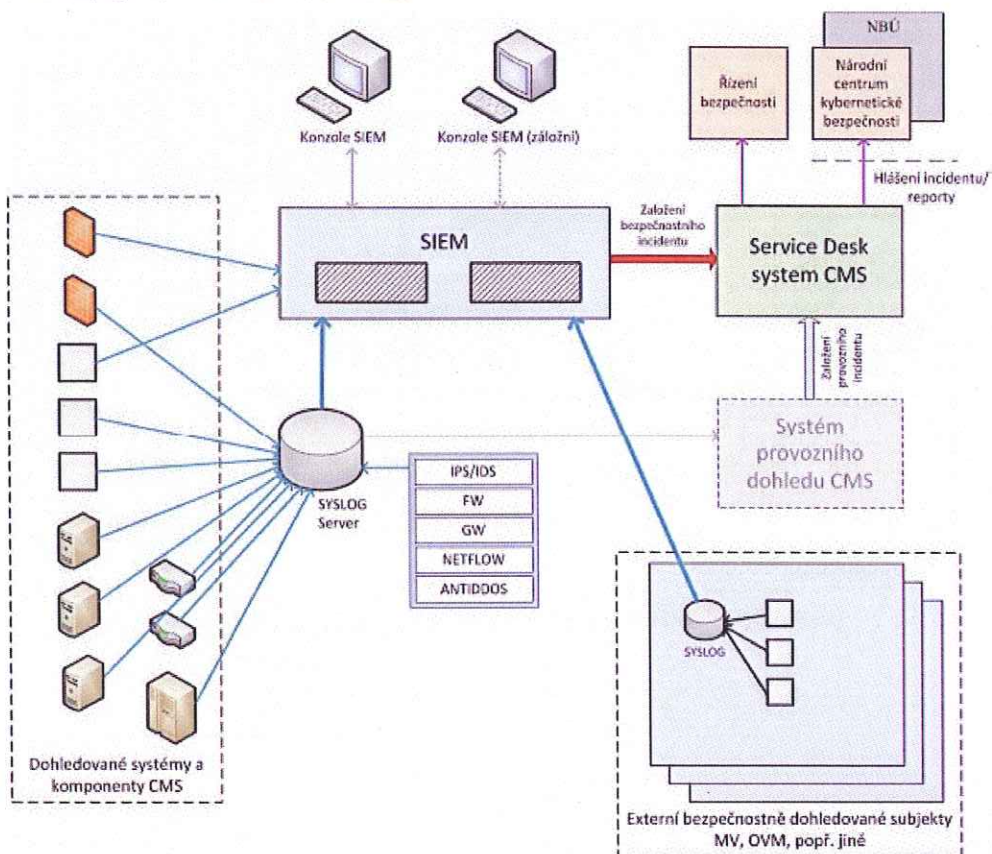
Uvedené rozložení v rámci dvou lokalit (DC1 a DC2) vychází z původního konceptu projektu CMS 2.0 realizujícího DR řešení (Disaster Recovery). DR řešení umožní rychlé zotavení, popř. nepřerušeni provozu i v případě výpadku celého jednoho datového centra. Tento koncept je použit i pro část představující rozšíření o SOCCR.

3.2.2 INTEGRACE CENTRÁLNÍHO BODU BEZPEČNOSTI SIEM

Systém SIEM, který tvoří jádro bezpečnostního řešení pro CMS 2.0, může rozšířením konfigurace a navýšením kapacity pokrýt další systémy MV a OVM, které komunikují přes CMS, nebo zde může být tato komunikace propagována.

Existuje definovaný proces sběru bezpečnostních událostí a jejich korelace s ostatními událostmi odděleně od provozních dat. Data jsou sbírána z jednotlivých koncových zařízení jak CMS, tak i ostatních subjektů. Dále jsou doplněna o informace z dalších bezpečnostních systémů, především IPS/IDS, NBA – Netflow, Vulnerability scanneru a dalších. Dále dochází k jejich převodu na jednotný formát a jsou bezpečně uložena a následně vzájemně porovnávána. Data jsou dále interpretována v grafickém prostředí a poskytují ucelený přehled o bezpečnostní situaci v reálném čase pracovníkům řídicího a dohledového centra.

V případě vzniku bezpečnostního incidentu existuje úzká vazba na servicedesk. V řídicím centru existuje možnost doplnění o informace provozního charakteru a vyhodnocení relevantnosti. Odpovídající incidenty se budou reportovat do NCKB (Národní centrum kybernetické bezpečnosti) a zde se přijímají i oznámení vydané NBU.

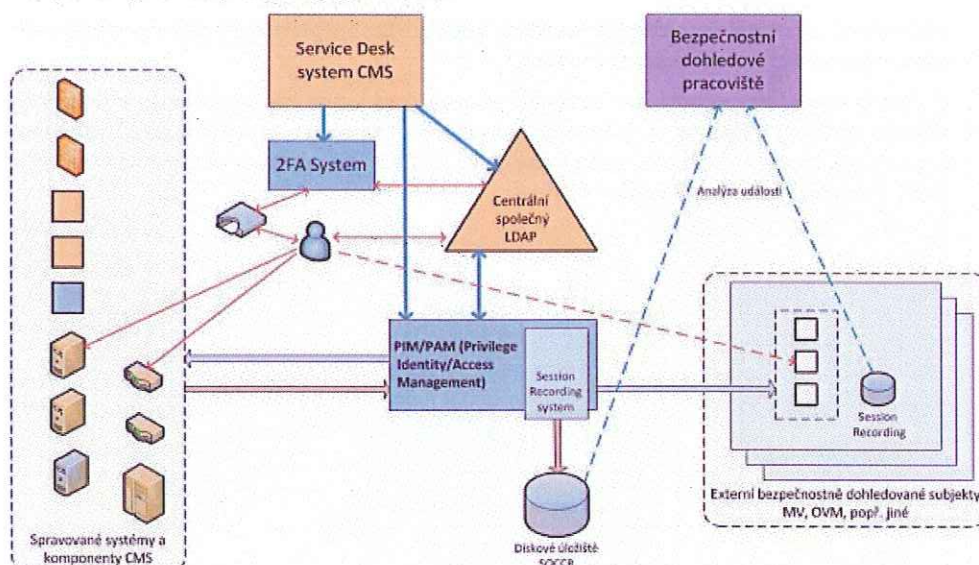


Obrázek 4 – Integrace SIEM

Projektový a investiční záměr, verze 1.4

3.2.3 INTEGRACE SYSTÉMU AUTENTIZAČNÍ PODPORY

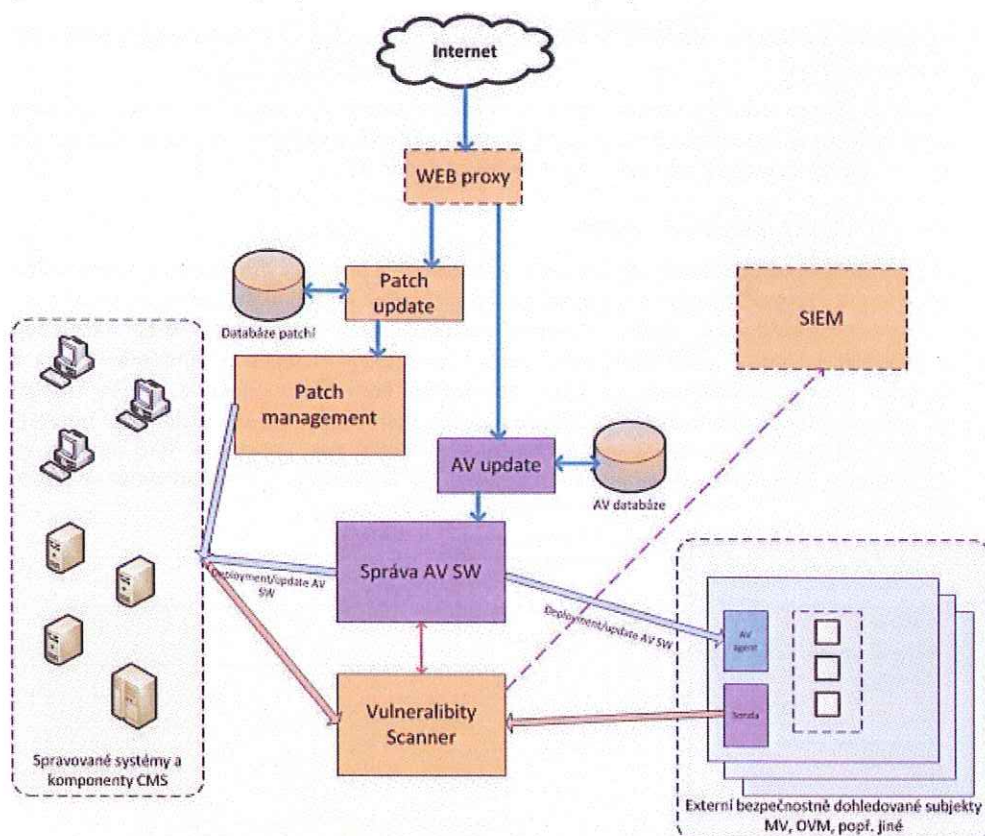
Systém autentizační podpory pro privilegované operace doplněný o dvoufaktorovou autentizaci znamená výrazné povýšení bezpečnosti celého CMS. Původní autentizace vyhovovala běžným bezpečnostním standardům. Nový návrh řešení se nyní dotýká oblasti vysoce bezpečné konfigurace a správy s provozbou na řídicí a dohledové centrum (SOCCR). Zabezpečené a sledované konfigurační sezení (sessions) mají jednorázovou platnost a zajišťují explicitní provedení změn. Řešení poskytuje služby vybraným komponentám jednak v CMS i mimo něj a integruje do svých procesů servicedeskové služby pro přihlášení uživatelů a zároveň je spojeno do hlavní bezpečnostní komponenty, kterou představuje jádro SIEM.



Obrázek 5 – Integrace systému autentizace

3.2.4 INTEGRACE ANTIVIROVÉHO ŘEŠENÍ A ŘÍZENÍ TECHNICKÝCH ZRANITELNOSTÍ

Antivirové řešení navržené v CMS je doplněno o další komponenty tak, aby se vytvořil vícevrstvý systém tvořený různými technologiemi a společně pokrývající jednak oblast perimetru, ale i samotné platformy operačních systémů. Celé řešení je tedy komplexní AV systém s centrálním managementem poskytující informace o aktuálním stavu virových hrozeb prostředí, doplněný o vektor zranitelnosti. Obě složky jsou dále stejným způsobem integrovány do jádra bezpečnostního řešení – SIEM, napojeny do dohledového a řídicího centra a poskytují služby prvkům uvnitř i vně CMS, resp. infrastruktura není členěna projektově.



Obrázek 6 – Integrace antiviru a skeneru technických zranitelností

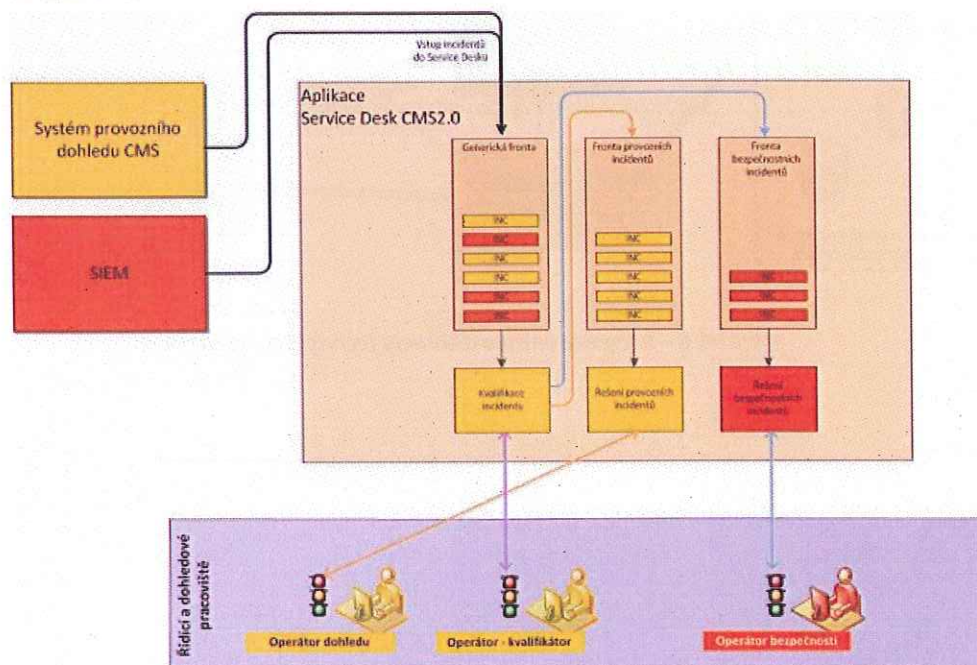
3.3 POPIS ARCHITEKTURY DOHLEDOVÉHO CENTRA

Sběr jednotlivých dat provozního a bezpečnostního dohledu bude probíhat samostatně, včetně dalších procesů probíhajících nad daty. Integrace na této úrovni je prováděna vzájemným křížovým poskytováním údajů, které mohou být relevantní pro obě strany (oba dohledy) a společným řídicím a dohledovým pracovištěm. To ve svém důsledku znamená, že provozní data bezpečnostní povahy mohou být předávána, vyhodnocena a eskalována na straně řešení SOCCR a s informacemi o bezpečnostních událostech může provozní dohled v rámci CMS 2.0. Přidaná hodnota spočívá ve využití synergického efektu, kdy budou sledovány provozní i bezpečnostní události komplexně a případné incidenty budou identifikovány a efektivně vyhodnocovány s minimálními časovými nároky.

Uvedený přístup rovněž procesně zajistí, že incidenty provozního charakteru mohou být následně překvalifikovány na incident bezpečnostní (pomocí nástrojů korelačních analýz apod.), což zabrání situaci, kdy by takováto skrytá aktivita mohla být přehlédnuta.

3.3.1 ŘÍDÍCÍ A DOHLEDOVÉ CENTRUM

Řídicí a dohledové centrum bude umístěno ve společném prostoru, kde budou zakončeny konzole provozních i bezpečnostních technologií poskytující celkový i jednotlivý pohled v aktuálním čase s možností doplňkových analýz. Výhodou takového řešení je rovněž větší akceschopnost dohledového týmu a maximálně rychlá reakce na případnou událost (odhalená aktivita často vyžaduje reaktivní zásah např. na úrovni zablokování komunikace útočníka, změny konfigurace síťového prvku či firewallu, zásah do systému apod.). Bude možné vzájemné doplnění provozních a bezpečnostních událostí za účelem zpřesnění identifikace typu incidentu. Tyto postupy budou zapracovány v procesech řízení incidentů a stejně tak bude upraveno workflow servicedesku, viz obrázek níže.



Obrázek 7 – Integrace řídicího dohledového centra



3.3.2 OSTATNÍ SYSTÉMY

Další dodatečné systémy bezpečnostního řešení budou integrovány stejným způsobem, infrastrukturně však neznamenaají výrazný zásah do koncepce uspořádání HW. Z tohoto pohledu jde o standardní aplikace provozované např. jako samostatný SW běžící na OS na virtualizované platformě.

3.4 KAPACITNÍ POŽADAVKY SOCCR (ROZŠÍŘENÍ CMS)

Rozšíření bezpečnostní struktury sebou nese kromě rozšíření o vlastní kapacitní náklady i další kapacitní vícenáklady v důsledku napojení všech komponent bezpečnostní infrastruktury do provozního dohledu. Dle předběžných výpočtů se celkové navýšení kapacit odráží v následujících parametrech uvedených v tabulce.

Služba	TB	CPU	RAM	Virt Srv
PIM+2FA	9,0	64	64	16
Provozní dohled	4,0	64	128	32
SIEM	17,0	32	64	16
AV+VULN	1,0	16	32	8
Archivace, zálohování ¹	45,0	10	64	4
Ostatní	5,0	16	32	8
CELKEM	81,0	202	384 GB	84

Tabulka 1: Kapacitní požadavky

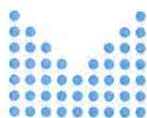
Infrastruktura SOCCR je plánována s rezervou, který pokryje připojení i dalších systémů MV a zpracovávání jejich dat provozního a bezpečnostního dohledu. Infrastruktura je připravena tak, aby v následných fázích po zahájení provozu bylo možné technologie (modulárně) rozšířit dle aktuálních potřeb a požadavků v závislosti na stavu CMS, připojených systémů a množství zpracováváných dat. Požadavky na rozšíření budou řešeny individuálně podle aktuálních potřeb. Zařízení SOCCR bude umístěno ve stejných prostorách jako zařízení CMS.

3.5 FÁZE INTEGRACE

Etapa propojení CMS a SOCCR začíná vlastní implementací bezpečnostní infrastruktury v souvislosti s implementací celého CMS. S tím souvisí doplnění a navýšení stávajících plánovaných kapacit v první fázi tak, aby mohlo dojít následnému rozšíření o požadované komponenty, které jsou na ní závislé.

V dalších fázích budou implementována bezpečnostní řešení do již kapacitně konsolidované infrastruktury. Integrace bude dále vyžadovat HW a vybavení řídicího a dohledového centra zřízeného v prostorách MV, včetně odpovídajících kapacit a nároků na lidské zdroje.

¹ Disková kapacita pro archivaci a zálohování je určena i pro další potřeby CMS (nejen pro SOCCR)



Projektový a investiční záměr, verze 1.4

3.6 PŘEDPOKLÁDANÝ HARMONOGRAM

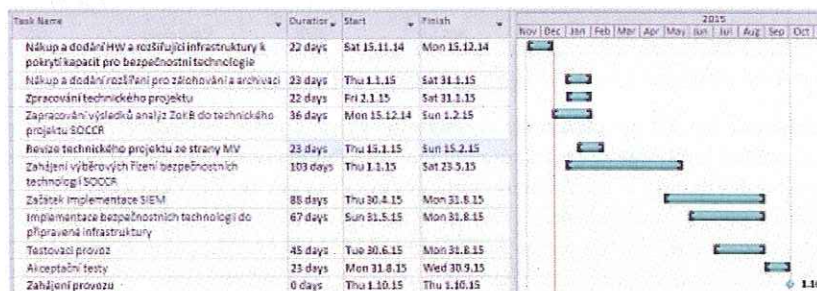
Harmonogram integrace je vázán na harmonogram CMS 2.0 a jeho jednotlivé milníky. S posunem termínu v projektu CMS 2.0 dojde i k posunu v projektu integrace.

Ve fázi 1, která začíná investicí v roce 2014, bude rozšířena kapacita virtualizační platformy, diskového pracovního prostoru a zálohovacích a archivačních služeb tak, aby pokryla potřeby bezpečnostních technologií propagovaných ve fázi 2. Výstupem z první fáze bude technický projekt, který bude detailně popisovat implementaci navržených technologií SOCCR a bude stanovovat rozsah parametrů servisní platformy, které jsou požadované pro projekty ITS NGN, KSP, NIS IZS, vč. cenového rozpočtu, který bude nutný pro finální stav provozního dohledu servisní platformy.

Fáze 2 představuje implementaci bezpečnostních technologií do připravené infrastruktury a znamená licenční navýšení prostředků provozního dohledu.

V následných fázích po zahájení provozu mohou být technologie rozšiřovány dle aktuálních potřeb a požadavků v závislosti na stavu CMS, připojených systémů a množství zpracovávaných dat. Jedná se pravděpodobně především o dopad na systém SIEM a Vulnerability management. Zde se dají předpokládat minimálně navýšení licenční. Rozpočet na rozšíření bude řešen individuálně podle aktuálních potřeb.

Níže uvedený harmonogram je navržený na aktuální stav projektu CMS 2.0. Jeho změny mohou ovlivnit i harmonogram dohledového centra SOCCR. Detailní harmonogram bude zpracován v rámci technického projektu SOCCR (1Q 2015).



Obrázek 8 – Předpokládaný harmonogram SOCCR

3.7 CERTIFIKACE ISMS

Dohledové centrum SOCCR je navrženo tak, aby splňovalo požadavky při budoucí certifikaci ISMS dle normy ISO/IEC 27001. Předpokládaný termín certifikace je předběžně určen na rok 2016. Soulad všech procesů, dokumentace i technologií s nejlepšími praktikami, které reprezentuje řada norem ISO 27k, je jednoznačným parametrem pro vybudování centra SOCCR.

3.8 UMÍSTĚNÍ ZAŘÍZENÍ SOCCR

Technologie a nástroje dohledového centra SOCCR budou integrální součástí Centrálního místa služeb, a proto i fyzické umístění zařízení bude shodné. Datová centra, kde jsou umístěna aktiva CMS, budou mít dostatečné zdroje pro umístění aktiv SOCCR. Za předpokladu, že provozovatelem SOCCR bude ČPOZ, bude řídicí a dohledové pracoviště umístěno v lokalitě Kodaňská 46 a/nebo Olšanská 4.

Projektový tým CMS 2.0 a SOCCR je složen ze stejných pracovníků ČPOZ, a proto budou při implementaci SOCCR všechny činnosti efektivně synchronizovány s činnostmi v rámci projektu CMS



2.0. Detailní plán implementace bude součástí Technického projektu SOCCR, který bude vytvořen v 1Q 2015.

3.9 RÁMCOVÝ ROZPOČET

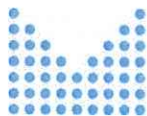
Investice do dohledového centra SOCCR je v celkové výši přesahující 50 mil Kč. Položkový rozpočet uvedený níže obsahuje předpokládané částky, které jsou nicméně závislé na výsledcích jednotlivých výběrových řízení. Část HW infrastruktury může být nakoupena v roce 2014 na základě již uzavřených rámcových smluv. Většina celkového řešení bude zainvestována v roce 2015.

Položka	Počet	CAPEX za jednotku	CAPEX celkem	Poznámka	OPEX 2015 (od září)	OPEX 2016	OPEX 2017	OPEX 2018
Diskové pole 100 TB	4	3 100 000 Kč	12 400 000 Kč	Rámcová smlouva uzavřena, možné nakoupit. Podpora na 5 let je zahrnuta v ceně.				
Blade servery	40	120 000 Kč	4 800 000 Kč	Rámcová smlouva uzavřena, minimálně 30 dní. Podpora na 5 let je zahrnuta v ceně.				
Virtualizační SW, instalace	40	100 000 Kč	4 000 000 Kč	Rámcová smlouva uzavřena, minimálně 30 dní. Podpora na 5 let je zahrnuta v ceně.				
Rízení privilegovaných přístupů (PIM/PAM)			3 310 000 Kč	Výběrové řízení 2015	99 300 Kč	331 000 Kč	331 000 Kč	331 000 Kč
Základní modul, licence enterprise bez omezení počtu systémů, 50 administrátorů, 1Y warranty	1	1 400 000 Kč	1 400 000 Kč					
Session recording module, 10 konkurent nahrávaných session	1	800 000 Kč	800 000 Kč					
DR/HA module (High Availability)	1	300 000 Kč	300 000 Kč					
Implementace (MD subdodavatel)	30	17 000 Kč	510 000 Kč					
Školení administrátorů MV	20	15 000 Kč	300 000 Kč					
Řešení pro dvoufakt. autentizaci			1 110 000 Kč	Výběrové řízení 2015	33 300 Kč	111 000 Kč	111 000 Kč	111 000 Kč
Licence pro administrátory systémů (rozšíření PIM/PAM)	50	12 000 Kč	600 000 Kč					
Implementace (MD subdodavatel)	30	17 000 Kč	510 000 Kč					
Archivační SW (5 TB)	25	55 000 Kč	1 375 000 Kč	Rámcová smlouva bude podepsána v 12/2014. Podpora na 5 let je zahrnuta v ceně.				
Zálohovací SW (5 TB)	15	335 000 Kč	5 025 000 Kč	Rámcová smlouva bude podepsána v 12/2014. Podpora na 5 let je zahrnuta v ceně.				
Rozšíření servisní platformy pro NIS, KSP, ITS (ServiceDesk, prov. monitoring, billing, provisioning...)			5 945 000 Kč	Rámcová smlouva bude podepsána v 2/2015	133 350 Kč	444 500 Kč	444 500 Kč	444 500 Kč
Licence ITS	92	35 000 Kč	3 220 000 Kč		96 600 Kč	322 000 Kč	322 000 Kč	322 000 Kč
Licence NIS	12	35 000 Kč	420 000 Kč		12 600 Kč	42 000 Kč	42 000 Kč	42 000 Kč
Licence KSP	23	35 000 Kč	805 000 Kč		24 150 Kč	80 500 Kč	80 500 Kč	80 500 Kč
Implementace (MD subdodavatel)	100	15 000 Kč	1 500 000 Kč					
Antivirus			800 000 Kč	Výběrové řízení 2015	24 000 Kč	80 000 Kč	80 000 Kč	80 000 Kč
Licence (servery)	50	10 000 Kč	500 000 Kč					
Implementace (MD subdodavatel)	20	15 000 Kč	300 000 Kč					
Honeypot			350 000 Kč	Výběrové řízení 2015	10 500 Kč	35 000 Kč	35 000 Kč	35 000 Kč
HW/SW Honeypot	2	100 000 Kč	200 000 Kč					
Implementace (MD subdodavatel)	10	15 000 Kč	150 000 Kč					
Rídící a dohledové pracoviště			1 616 000 Kč	Výběrové řízení 2015	48 480 Kč	161 600 Kč	161 600 Kč	161 600 Kč
HW vybavení (LCD, PC/NB)	8	40 000 Kč	320 000 Kč					
Systém velkých obrazovek	6	50 000 Kč	300 000 Kč					
Školící a testovací místnost (LCD, PC/NB)	10	40 000 Kč	400 000 Kč					
Projektor	2	18 000 Kč	36 000 Kč					
Interaktivní tabule	1	60 000 Kč	60 000 Kč					
Síťové technologie, aktivní prvky (soubor)			500 000 Kč					
Nástroj pro řízení rizika BCM			1 260 000 Kč	Výběrové řízení 2015	37 800 Kč	126 000 Kč	126 000 Kč	126 000 Kč
Aplikace pro řízení rizik a BCM	1	1 100 000 Kč	1 100 000 Kč					
Implementace, školení	4	40 000 Kč	160 000 Kč					
Zpracování technického projektu			4 808 000 Kč					
Specialista bezpečnosti ICT (bezpeč. architekt)	110	14 300 Kč	1 573 000 Kč					
Bezpečnostní manažer	70	17 000 Kč	1 190 000 Kč					
Architekt řešení	110	15 500 Kč	1 705 000 Kč					
Analýtik BCM (Business Continuity)	20	17 000 Kč	340 000 Kč					
Projektové řízení a administrace			2 500 000 Kč					
Projektový manažer senior	80	13 000 Kč	1 040 000 Kč					
Projektový administrátor	120	10 000 Kč	1 200 000 Kč					
Manažer kvality	20	13 000 Kč	260 000 Kč					
Implementace technologií			6 814 000 Kč					
Specialista bezpečnosti ICT	180	14 300 Kč	2 574 000 Kč					
Bezpečnostní manažer	140	17 000 Kč	2 380 000 Kč					
Administrátor systémů	120	15 500 Kč	1 860 000 Kč					
Předpokládané personální zajištění provozu SOCCR	4				1 680 000 Kč	5 600 000 Kč	5 600 000 Kč	5 600 000 Kč
Celkem			56 113 000 Kč		2 066 730 Kč	6 889 100 Kč	6 889 100 Kč	6 889 100 Kč

Všechny ceny jsou uvedeny vč. DPH

Tabulka 2: Předpokládaný rozpočet SOCCR²

² Podpora na 5 let pro diskové pole, servery, virtualizaci a zálohování je součástí investice



Projektový a investiční záměr, verze 1.4

Rozpočet přesahuje předem plánovaný strop investičních nákladů ve výši 50 mil, protože je založen na předpokládaných cenách řešení, které mohou být sníženy v rámci výběrových řízení. Pořadí jednotlivých položek určuje prioritu nákupu (vyjma personálních nákladů na provoz a implementaci). Částky vyplývají z předpokládaných cen pro jednotlivá výběrová řízení a jsou určeny jako v místě a čase obvyklé. Cenový odhad u položek s odkazem na rámcovou smlouvu vychází z již vysoutěžených cen. Některé smlouvy budou podepsány až v příštích měsících, proto je možné definitivně potvrdit přesné ceny až po podepsání těchto smluv.

Personální zajištění pro provoz dohledové centra 2014 je předpokládáno 4 FTE od zahájení provozu v září/říjnu 2015. Výběrová řízení obsahují požadavky na školení jednotlivých technologických platforem a provozních rolí. Výběrová řízení budou realizována v souladu se zákonem 137/2006 o veřejných zakázkách a podle pravidel dotačních programů, aby bylo možné využít v případě vhodné výzvy zpětného financování z evropských fondů.

Součástí finančního rozpočtu SOCCR jsou náklady na část technologií, nástrojů a vybavení dohledového centra. Kritické a významné systémy MV, které budou dohledovány, mohou na své straně vyžadovat změny, jež nejsou financovány v rámci projektu SOCCR. Odhad těchto nákladů je individuální záležitostí jednotlivých systémů.



4 SEZNAM ZKRATEK

Zkratka	Vysvětlení
AIS	Automatizovaný informační systém
BCM (Business Continuity Management)	Oblast řízení, která je zaměřena na to, aby byly trvale dostupné všechny kritické funkce organizace vůči zákazníkům, dodavatelům a dalším stranám
CMS	Centrální místo služeb
ČPOZ	Česká pošta s.p., odštěpný závod ICT Služby
ČR	Česká republika
DC	Datové centrum
DR (Disaster Recovery)	Předem připravený scénář, který vede k obnově infrastruktury po nastalé havárii
FTE (Full Time-Equivalent)	Ukazatel jež vypovídá o stupni zapojení zaměstnance na projektu
HoneyPot	Informační systém, který emuluje chod standardních systémů nebo sítí. Slouží k včasnému odhalení neoprávněné komunikace
HW	Hardware
IPS/IDS (Intrusion Prevention / Deception System)	Systém pro prevenci nebo detekci průniku do sítě
ISMS (Information Security Management System)	Systém řízení a správy informačních aktiv
ITS NGN	Integrovaná telekomunikační síť MV
KSP	Krajské standardizační projekty NIS IZS
MV	Ministerstvo vnitra
NBA-Netflow (Network Behavioral Analysis)	Analytický nástroj pro zjištění chování sítě
NBU	Národní bezpečnostní úřad
NCKB	Národní centrum kybernetické bezpečnosti
NIS ISZ	Národní informační systém integrovaného záchranného systému
OS	Operační systém
OVM	Orgán veřejné moci
SIEM (Security Incident & Event Management)	Systém pro správu událostí a řízení bezpečnosti
SOCCR (Security Operation Center for Continuous Reliability)	Dohledové centrum SOCCR
SW	Software
ZoKB	Zákon o kybernetické bezpečnosti



Specifikace požadavků na technický projekt

Předpokládaný rozsah dokumentu: cca 150 stran

1. Terminologie a zkratky
2. Rámcový popis navrhovaného řešení Dohledového centra MV
 - 2.1. Provozní dohled
 - 2.2. Bezpečnostní dohled
3. Celková architektura
 - 3.1. Hardwarová architektura
 - 3.2. Softwarová architektura
4. Legislativní požadavky
 - 4.1. Provozní dohled
 - 4.2. Bezpečnostní dohled
5. Dostupnost řešení
6. Definování služeb
 - 6.1. Katalog služeb
 - 6.2. Sledován plnění služeb
7. Konceptuální architektura
8. Organizační zajištění
 - 8.1. Organizační model
 - 8.2. Definování rolí a odpovědností
 - 8.3. Komunikační model
9. Analýza okolí
 - 9.1. Identifikace externích systémů a definování rozhraní
 - 9.2. Definice modulárního rozvoje dohledového centra
10. Funkční model/Use Case diagram
11. Procesní model
 - 11.1. Provozní dohled
 - 11.2. Bezpečnostní dohled
12. Integrační rozhraní
 - 12.1. Servicedesk
 - 12.2. Provozní dohled
 - 12.3. Bezpečnostní dohled
13. Plán integrace řešení
 - 13.1. Etapizace integrace provozního dohledu
 - 13.2. Etapizace integrace bezpečnostního dohledu
14. Management a monitoring
 - 14.1. Provozní dohled
 - 14.2. Bezpečnostní dohled

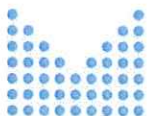


- 15. Archivace a zálohování
 - 15.1. Provozní dohled
 - 15.2. Bezpečnostní dohled
 - 15.3. Servicedesk
- 16. Plán testování
 - 16.1. Metodika testování
 - 16.2. Rozsah testování
 - 16.3. Plán testování
- 17. Provoz navrženého řešení
 - 17.1. Testovací prostředí
 - 17.2. Dohledové centrum
 - 17.3. Bezpečnostní dohled
 - 17.4. Service desk
 - 17.5. Provozní dokumentace
 - 17.6. Zálohování a archivace
 - 17.7. Požadavky na provoz
 - 17.8. Nacenění provozních požadavků
- 18. SLA
- 19. Reporting
- 20. Podrobný položkový rozpočet
- 21. Harmonogram vytvoření provozní dokumentace
- 22. Závěry a doporučení
- 23. Přílohy



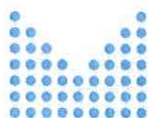
Harmonogram plnění

	Část Díla	Zahájení	Ukončení
1	Technický projekt	1. 1. 2015	31. 3. 2015
2	Realizace výběrových řízení a dodávka HW a SW	1. 4. 2015	30. 6. 2014
3	Vytvoření Dohledového centra	1. 7. 2015	30. 11. 2015



Stanovené ceny MD (limitní ceny pro jednotlivé pracovní pozice)

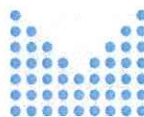
Role (pracovní pozice)	Cena za 1 člověkodenní v Kč bez DPH
Specialista bezpečnosti ICT (bezpečnostní architekt)	14.300,-
Bezpečnostní manažer	17.000,-
Architekt řešení	15.500,-
Analytik BCM (Business Continuity)	17.000,-
Projektový manažer senior	13.000,-
Projektový administrátor	10.000,-
Manažer kvality	13.000,-
Administrátor systémů	15.500,-



Metodika projektového řízení

Obsah dokumentu:

1. METODIKA PROJEKTOVÉHO ŘÍZENÍ	2
1.1. Základní ustanovení	2
1.2. Zúčastněné strany projektu	2
2. VÝKLAD POJMŮ	3
3. POUŽITÉ ZKRATKY	7
4. PROJEKT DOHLEDOVÉ CENTRUM MV PRO PROVOZ ICT SYSTÉMŮ A KYBERNETICKOU BEZPEČNOST (SOCCR)	8
4.1. Závaznost projektových standardů	8
4.2. Standardní náležitosti dokumentů	8
4.3. Úložiště projektové dokumentace	8
4.4. Cíle Projektu	9
4.5. Popis fází Projektu (Životní cyklus Projektu)	10
4.6. Řízení a organizace Projektu	11
4.7. Akceptace	26
4.8. Issue Management	31
4.9. Záruky	33
4.10. Ostatní	34
5. OBSAZENÍ PROJEKTU NA STRANĚ DODAVATELE	34
6. ETAPY PLNĚNÍ A AKCEPTAČNÍ KRITÉRIA	34
6.1. Etapy plnění	35
6.2. Akceptační kritéria	35
6.3. Vzor akceptačního protokolu	36
7. ŘÍZENÍ RIZIK	37
7.1. Řízení rizik	37
7.2. Reportování a monitorování rizik	38
7.3. Návrh registru rizik	40



1. Metodika projektového řízení

1.1. Základní ustanovení

Účelem tohoto dokumentu je definice metodiky řízení části projektu „Dohledové centrum MV pro provoz ICT systémů a kybernetickou bezpečnost (SOCCR)“ (dále jen „**Projekt**“). Cílem je vymezit projektové přípravy Projektu, řídicí a organizační struktury Projektu, postupy, metodiky, nástroje, techniky a závaznou projektovou dokumentaci.

Projektová metodika je soubor dohodnutých součinnostních pravidel a personálních struktur Objednatele a Dodavatele, podle kterých jednají s cílem zajistit odevzdání bezvadného díla v dohodnutém termínu. Tato metodika se pro obě strany závazně vztahuje na časový úsek od nabytí účinnosti Smlouvy o dílo do jeho bezvadného odevzdání a akceptace Objednatelem.

1.2. Zúčastněné strany projektu

Dodavatelem pro tento Projekt je společnost Česká pošta, s.p., Odštěpný závod ICT služby (dále jen „**Dodavatel**“) a objednatel tohoto Projektu je Česká republika – Ministerstvo vnitra (dále jen „**Objednatel**“).

1.2.1. Platnost a závaznost

Dodržování pravidel a ustanovení definovaných v této Metodice projektového řízení je závazné v průběhu celého Projektu. V průběhu realizace Projektu může být v případě potřeby tato Metodika Projektového řízení aktualizována či upřesněna, a to po dohodě všech zúčastněných stran.

Dodržování definovaných postupů a pravidel je po schválení této Metodiky projektového řízení povinností všech stran zúčastněných na Projektu. Při nedodržení závazného pravidla některou zúčastněnou stranou jsou zbývající strany oprávněny požadovat nápravu u té strany, která pravidlo porušila. Strana, která nedodržela závazné pravidlo a byla na to upozorněna, je povinna neprodleně provést nápravu v souladu s touto Metodikou projektového řízení.

Metodika projektového řízení nabývá platnosti oficiálním schválením smluvními stranami. Toto schválení je provedeno formou podpisu tohoto dokumentu.

1.2.2. Odpovědnosti

Za dodržování a prosazování zde uvedených pravidel jsou zodpovědní vedoucí Projektu (dále jen „**PM**“) každé zúčastněné strany Projektu.

1.2.3. Odkaz na Smlouvu

Tato Metodika projektového řízení navazuje na Smlouvu o dílo na vytvoření Dohledového centra ministerstva vnitra pro provoz ICT systémů a kybernetickou bezpečnost (dále jen „**Smlouva**“) uzavřenou mezi Dodavatelem a Objednatelem a definuje postupy a pravidla, která budou uplatňována za účelem dodávky předmětu plnění této Smlouvy.



2. Výklad pojmů

Pojem	Popis
Akceptace	Akt přijetí výstupu (dodávky) Projektu, nebo jeho části, s jednoznačným uznáním, že byl dodán přesně tak, jak dodán být měl. Vlastní Akceptace výstupu (dodávky) je výsledkem procesu Akceptace, v jehož rámci je dodávané Dílo předáno Objednateli a je dohodnuta přiměřená lhůta pro akceptování díla relevantními pracovníky Objednatele. (Proces Akceptace může být i několikakolový, zejména v případě, kdy jsou v průběhu akceptačního procesu objeveny překážky, které Akceptaci Díla brání a musí být proto odstraněny). Závěrem procesu Akceptace je vždy podepsání Akceptačního protokolu na dodávku Projektu.
Akceptační kritéria	Seznam kritérií seřazený podle priorit. Tato kritéria musí finální produkt splnit před svým přijetím (akceptací) Objednatелеm; měřitelná definice toho, co je třeba udělat pro to, aby bylo Dílo akceptovatelné klíčovými zainteresovanými stranami.
Akceptační protokol	Formální dokument, který stvrzuje Akceptaci výstupu (dodávky) Projektu. Podpisem tohoto dokumentu potvrzuje Objednatel, že Projekt byl dokončen a dodán přesně podle jeho kritérií, měřítek a základních podmínek, která měla být dodržena. Akceptační protokol je právním uznáním kompletnosti a správnosti dodávky.
Analýza	Rozbor, metoda zkoumání složitějších skutečností rozkladem na jednodušší (postup od abstraktního ke konkrétnímu).
Audit	Systematický, nezávislý a dokumentovaný proces pro objektivní získání a vyhodnocení důkazů týkajících se provádění činností, s cílem zjistit míru souladu mezi zjištěnými informacemi o provádění činností a stanovenými kritérii.
Část	Část Projektu je technicky, finančně a časově nezávislá fáze plnění, která je logicky kontrolovatelná a samostatně akceptovaná a po níž může být proplacena část ceny díla. Projekt sestává z jediné nebo z více částí. Části musí na sebe časově navazovat (tj. nesmí se překrývat a ani nesmí být přerušeny).
Etapa	Část Projektu je technicky a časově nezávislá fáze plnění, která je logicky kontrolovatelná a samostatně akceptovaná. Projekt sestává z jediné nebo z více etap. Etapy na sebe nemusí časově navazovat (tj. může jich souběžně běžet několik a mohou být přerušeny).
Harmonogram Projektu	Grafické znázornění plánu (například Ganttovým diagramem), popisující posloupnost úkolů, společně s přidělením zdrojů, které dohromady tvoří plán. V rámci projektového řízení by měly být projektové aktivity dokumentovány v harmonogramech spojených s Projektovým Plánem. Činnosti přiřazené na základě každodenního řízení mohou být dokumentovány v relevantních přehledech (tj. Registru rizik, Registru



Pojem	Popis
	otevřených problémů a Registru kvality), pokud nevyžadují významnou aktivitu.
Issue log	Dokument obsahující všechny požadavky (otevřené body) Objednatele nahlášené Dodavateli v průběhu Projektu, včetně jejich aktuálního stavu. Soupiska otevřených bodů by měla být pravidelně kontrolována Projektovým manažerem Objednatele i Projektovým manažerem dodavatele.
Kick-off Projektu	Úvodní schůzka Projektu, na které dochází k formálnímu zahájení Projektu a sdělení všech důležitých informací týkajících se typu a rozsahu Projektu, Objednatele a dalších zúčastněných partnerů, členům projektového týmu. Kick-off Projektu svolává příslušný Projektový manažer.
Kontrolní schůzka Projektu	Pravidelná schůzka za účasti pověřených zástupců Dodavatele a Objednatele, na které je detailně procházen pokrok dosažený do konce sledovaného období na Projektu a výhled do konce Projektu. Podkladem pro Kontrolní schůzku je vždy Zpráva o stavu Projektu pro Objednatele a výstupem je Zápis z Kontrolní schůzky. Kontrolní schůzka Projektu slouží obvykle i jako příprava na jednání ŘV.
Kontrola kvality	Proces monitorování specifických výsledků projektu s cílem určit, zda splňují relevantní standardy s cílem identifikovat způsoby, jak odstranit příčiny neuspokojivých výkonů.
Kritéria kvality	Popis specifikace kvality, kterou musí produkt splňovat a specifikace měřítek kvality, která budou uplatněna těmi, kteří kontrolují konečný produkt.
Kvalita	Celkový souhrn vlastností a odvozených nebo stanovených charakteristik produktu, osoby, procesů, služby a/nebo systému, které mají společně schopnost prokázat, že produkt splňuje očekávání nebo uspokojuje dané potřeby, požadavky nebo specifikace.
Metodika	Souhrn doporučených praktik a postupů, strukturovaně popisující celý ŽC určité entity a ukotvující co, kdo a jak má vykonat k dosažení stanoveného cíle Projektu.
Milník	Významná událost v rámci Projektu, ve které se měří rozpracovanost produktů. Milník představuje bod zpětné kontroly, bod přijetí rozhodnutí nebo body přejímky. Milník má v harmonogramu Projektu nulovou délku trvání.
Nabídka	Dokument, ve kterém potencionální Dodavatel nabízí dodat své služby/zboží ve stanoveném rozsahu, za stanovenou cenu a za stanovených podmínek. Vyjadřuje tím svůj zájem vstoupit do ujednání či smluvního vztahu s tím, komu Nabídku předkládá.
Pilotní provoz / Příprava předání do	Zkušební neboli ověřovací provoz systému – předmětu dodávky, včetně příp. migrace dat a zaškolení koncových uživatelů. Závěrem úspěšné fáze



Pojem	Popis
produkce	Pilotního provozu Objednatel přebírá uživatelskou a technickou dokumentaci a systém je předán do Ostrého provozu.
Plán Projektu	Plán zahrnující hlavní produkty Projektu, termíny dodání a výši nákladů. Původní Projektový Plán je předkládán jako součást dokumentace o nastavení Projektu. Plán je revidován, jakmile jsou k dispozici aktuální informace o postupu. Jedná se o hlavní kontrolní dokument pro Řídící výbor sloužící k měření skutečného postupu oproti očekávání.
Plán řízení kvality Projektu	Dokument definující příslušné standardy a postupy, které musí být v průběhu celého Projektu dodržovány proto, aby bylo možné Projekt úspěšně dodat v požadované kvalitě. Je součástí projektové dokumentace a je vypracován v průběhu procesu <i>Plánování Projektu</i> .
Popis role	Popisuje soubor odpovědností charakteristických pro danou roli.
Projektový manažer, PM	Specialista na oblast projektového managementu, který odpovídá za naplánování a dodávku daného Projektu na každodenní bázi. Jeho povinností je zajistit úspěšné dodání Projektu v požadované kvalitě, a to cestou minimalizace rizik v průběhu celého životního cyklu Projektu.
Pracovní instrukce	Detailní pokyny vydané jednotlivým členům Projektového týmu pro splnění určitých konkrétních úkolů na Projektu. Jsou součástí projektové dokumentace a vydává je PM v průběhu procesu <i>Kontrola Projektu</i> .
Proces	Strukturované kroky navržené pro dosažení konkrétních výsledků. Proces využívá jednoho nebo více definovaných vstupů a mění je v definované výstupy.
Produkt	Výrobek, vytvořená hodnota, výsledek činnosti (výstupy činnosti). Produkt může představovat souhrn dílčích subproduktů.
Produktivní provoz	Živý neboli ostrý provoz systému – předmětu dodávky, kdy je spuštěna příslušná funkcionálita v reálném (rutinním) provozu Objednatele.
Projekt	Jedinečný časově, nákladově a zdrojově omezený proces realizovaný za účelem vytvoření definovaných výstupů (rámeček naplnění projektových cílů) co do kvality, standardů a požadavků.
Projektový management	Proces uplatňování znalostí, odborných zkušeností, nástrojů a technik u širokého rozsahu projektových aktivit (zahrnujících plánování, organizování a řízení zdrojů), které jsou prováděny za účelem dodání určitého Projektu podle požadavků Objednatele.
Realizace	Vlastní implementace systému podle Technického projektu a příprava systému pro Pilotní (ověřovací) provoz.
Registr rizik	Záznam identifikovaných rizik, včetně jejich aktuálního stavu a historie. Nástroj používaný při plánování a realizaci Projektů, a to v rámci procesu řízení rizik. Slouží k identifikaci, analýze a vlastnímu řízení rizik každého Projektu. Obsahuje údaje o rizicích, která byla projektovým týmem



Pojem	Popis
	identifikována, jejich dopad na Projekt, výši jejich pravděpodobnosti, plán jejich eliminace a plán postupu pro případ, že skutečně nastanou.
Riziko	Riziko lze definovat jako nejistotou událost nebo soubor událostí, které pokud nastanou, budou mít dopad na dosažené cíle Projektu. Riziko je měřeno kombinací pravděpodobnosti uvědomění si hrozby nebo příležitosti a závažnosti jeho dopadu na cíle.
Rozsah (scope) Projektu	Rozsah plánu je součet jeho dílčích částí a rozsah jejich požadavků. Je popsán produktovým rozpadem pro plán a odpovídajícími popisy Díla.
Řešitelský tým	Osoby pracující na realizaci Projektu přímo podřízenému PM.
Řídící výbor, ŘV	Představuje nejvyšší orgán Projektu, který formálně akceptuje projektové výstupy, kontroluje a sleduje průběh Projektu a schvaluje změny Projektu. Je vrcholným rozhodovacím orgánem s primární úlohou udávat směr a zajišťovat rozhodování o Projektu. Členy ŘV jsou zástupci Objednatele i Dodavatele. Hlavní rozhodovací odpovědnost nese obvykle Sponzor Projektu na straně Objednatele, který je obvykle předsedou ŘV. V některých odůvodněných případech mohou být členy ŘV i Subdodavatelé.
Řízení kvality	Koordinovaná opatření pro řízení a kontrolu organizace v oblasti kvality.
Řízení rizik	Systematická aplikace principů, přístupů a procesů sloužící k identifikaci a hodnocení rizik a poté plánování a implementace reakcí na rizika.
Smlouva	Závazná dohoda dvou nebo více stran o dodávce služeb a/nebo zboží za konkrétních, ve Smlouvě zakotvených, podmínek. Má písemnou formu a je právně vymahatelná.
Sponzor Projektu	Nejedná se o specifickou roli v rámci projektového řízení, ale většinou se používá k označení hlavní hybné síly projektu. Může být ekvivalentem Sponzora projektu v projektovém řízení nebo vedení společnosti/programu. Do češtiny se překládá role „Executive“ a „Sponsor“ shodně slovem „Sponzor projektu“.
Studie proveditelnosti, Projektový a investiční záměr	Nejvyšší stupeň analýzy investičního záměru nebo podnikatelského záměru. Úvodní studie, jejímž cílem je určit zda je určité řešení realizovatelné. V rámci studie (záměru) je problém pojmenován, jsou identifikována jednotlivá řešení a navržena doporučení dalších kroků.
Subdodavatel	Právnícká či fyzická osoba najata Dodavatelem k provedení určité části Projektu formou dodávky Objednateli. Subdodavatel uzavírá Smlouvu s Dodavatelem a nemá přímý právní vztah s Objednatelem. Za výstupy Subdodavatele odpovídá Objednateli.
Subdodávka	Soubor aktivit, prováděných s cílem dodat určité části Projektu najatým Subdodavatelem. Výstupy dodané v rámci Subdodávky jsou Objednateli

Pojem	Popis
	dodány Dodavatelem jako součást Projektu a Dodavatel za ně také Objednateli odpovídá.
Vedení Projektu	Nejvyšší výkonný orgán Projektu. Má řídicí a rozhodovací pravomoc, v jejichž rámci provádí průběžné řízení Projektu a rozhoduje o postupu Projektu v mezích daných Smlouvou, Plánem Projektu a rozhodnutími ŘV.
Objednatel	Osoba nebo skupina zadávající Dílo, která bude těžit z koncového výstupu. Právnícká (nebo fyzická) osoba, se kterou je uzavřena Smlouva na dodávku určité služby a/nebo zboží.
Dodavatel	Právnícká nebo fyzická osoba, která dodává služby a/nebo zboží jiné právnícké nebo fyzické osobě podle podmínek daných uzavřenou Smlouvou.
Zpráva o stavu Projektu pro Objednatele	Formální pravidelná zpráva o stavu Části Projektu, kterou projektový manažer Dodavatele předkládá Objednateli. Obvykle je vystavován v pravidelných, nejčastěji měsíčních, periodách.
Životní cyklus Projektu	Logický sled aktivit, který je ohraničen začátkem a koncem projektu. Každý Projekt, bez ohledu na jeho rozsah a komplexnost, prochází v průběhu své existence řadou fází, které společně tvoří životní cyklus Projektu. Životní cyklus projektu je dle projektového řízení definován jako období od zahájení Projektu do předání dokončeného produktu těm, kteří ho budou provozovat a udržívat.

3. Použité zkratky

Pojem	Popis
ČP OZ	Česká pošta, s.p., Odštěpný závod ICT služby
HTP	Hlavní tým Projektu
HW	Hardware
ICT	Informační a komunikační technologie (Information and Communication Technologies)
MV	Česká republika – Ministerstvo vnitra
NPD	Následující pracovní den
PM	Project manažer/Vedoucí Projektu
RT	Realizační tým
ŘV	Řídící výbor
VP	Vedení Projektu
ŽC	Životní cyklus



Pojem	Popis
ZoKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů

4. Projekt Dohledové centrum MV pro provoz ICT systémů a kybernetickou bezpečnost (SOCCR)

Metodika řízení Projektů definuje povinné standardy, které stanovují pravidla vzniku, uložení a archivace projektové dokumentace.

4.1. Závaznost projektových standardů

Standardy Projektu musí odpovídat interním pravidlům řízení organizace. Jsou závazné pro všechny členy Projektu, jak ze strany Objednatele, tak Dodavatele, příp. i pro pracovníky třetích stran, kteří se podílejí na realizaci Projektu. Přičemž Dodavatel zodpovídá za potřebné seznámení s těmito standardy.

4.2. Standardní náležitosti dokumentů

Všechny projektové dokumenty musí splňovat:

- Každý dokument, který je součástí dokumentace Projektu, musí být označen jednoznačnou identifikací.
- Budou uloženy na sdíleném zabezpečeném serveru v projektové knihovně, do které budou mít po celou dobu trvání Projektu přístup dle nadefinovaných uživatelských práv.

4.3. Úložiště projektové dokumentace

Projektová dokumentace je uchovávána v elektronické i listinné podobě.

4.3.1. Projektová knihovna

Projektová knihovna je určena pro centrální správu projektové dokumentace v elektronické podobě.

Projektová knihovna je vytvořena a spuštěna v přípravné fázi Projektu. Za správu projektové dokumentace zodpovídá Dodavatel. Pravidla a přístupová práva do projektové knihovny definují projektoví manažeři smluvních stran. Přístupem k datům disponují pouze oprávněné osoby projektového týmu.

4.3.2. Projektový depozitář

Projektové dokumenty určené pro uchovávání v listinné podobě, je nutné archivovat fyzicky v místnosti s řízeným přístupem. Jedná se zejm. o archivaci podepsaných dokumentů Projektu.

Dodavatel je povinen archivovat originální vyhotovení Smlouvy včetně jejích dodatků, originály účetních dokladů a dalších dokladů vztahujících se k realizaci předmětu této Smlouvy po dobu 10 let od ukončení Projektu.

Projektovou dokumentaci spravuje projektový manažer Dodavatele, příp. administrátor Projektu.



4.4. Cíle Projektu

4.4.1. Hlavní cíle Projektu

Projekt Dohledové centrum MV pro provoz ICT systémů a kybernetickou bezpečnost (SOCCR) navazuje na projekty ITS NGN, KSP A NIS a je založen na Konceptu KIVS, která byla schválena usneseními vlády č. 1156, 1270 a 1453 z roku 2006. KIVS je navržena jako centralizovaná komunikační infrastruktura s Centrálním místem služeb (dále jen „CMS“), které je jediným místem výměny dat mezi jednotlivými informačními systémy (dále jen „IS“) veřejné správy (dále jen „ISVS“) a zároveň jediným místem propojení k veřejné síti internet a specifických neveřejných sítí např. sítí Evropské unie (dále jen „EU“).

Projekt Dohledové centrum MV pro provoz ICT systémů a kybernetickou bezpečnost (SOCCR) rozšiřuje funkčnost servisní platformy eGovernmentu v rámci Centrálního místa služeb a naplňuje požadavky zákona 181/2014 o kybernetické bezpečnosti. Dohledové centrum SOCCR je navrženo plně v souladu se schválenou Strategií kybernetické bezpečnosti na roky 2012 – 2015, stejně tak s budoucí, zatím neschválenou, strategií na roky 2015 – 2020 (ve fázi přípravy).

Přínosy a cíle projektu Dohledové centrum MV pro provoz ICT systémů a kybernetickou bezpečnost (SOCCR) jsou:

- naplnění technologických požadavků dle ZoKB pro definované systémy a síť MVČR
- zajištění provozního dohledu pro systémy a síť ITS NGN, KSP a NIS IZS

4.4.2. Faktory úspěchu Projektu

V rámci Projektu budou posuzovány následující faktory:

- Systém fungující v ostrém provozu od 31. 12. 2015, a to v rozsahu funkcionalit daných platnou Smlouvou, resp. Technickým projektem.
- Dodržení plánovaných termínů dokončení jednotlivých Částí Projektu.
- Písemná akceptace všech Částí Projektu.

4.4.3. Rizika Projektu

- Přehled hlavních rizik, která budou na Projektu identifikována, a plán jejich ošetření (eliminace) budou evidována v samostatném dokumentu Registr rizik, který bude pravidelně předkládán, jako příloha Zprávy o stavu projektu Vedení projektu. Dokument Registr rizik spravuje projektový manažer Dodavatele, příp. administrátor Projektu.

4.4.4. Omezení realizace

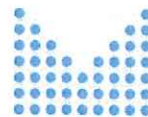
- Definice identifikovaných omezení a souvislostí, se kterými se musí při realizaci Projektu počítat. Toto může zahrnovat např. jiné probíhající projekty, jejichž ukončení musí jednoznačně předcházet začátku tohoto Projektu, nebo některé jeho fáze.
- Omezení realizace budou v případě potřeby eskalovány na Vedení projektu a následně budou zakomponována do Registru rizik.

4.5. Popis fází Projektu (Životní cyklus Projektu)

- Každý Projekt prochází od okamžiku svého vzniku několika fázemi, které společně tvoří tzv. Životní cyklus Projektu. Každá fáze má v projektu svou důležitou roli, je specifická svým cílem a výstupy a zanedbání některé z nich může později vést k závažným problémům nebo ke kolapsu celého Projektu právě proto, že nebyly dostatečně prozkoumány jednotlivé okolnosti a vlivy.
- Základní životní cyklus je stejný u všech Projektů, i když konkrétní průběh jednotlivých etap životního cyklu se obvykle liší, zejména v závislosti na typu a rozsahu dodávaných prací, typu a velikosti Objednatele a počtu a typu Subdodavatelů či dalších zúčastněných partnerů.
- Životní cyklus Projektu se skládá se z následujících fází:



Obr. č. 1 – Základní schéma Životního cyklu Projektu



4.6. Řízení a organizace Projektu

4.6.1. Popis a kompetence orgánů Projektu

Organizace celého Projektu je založena na společné práci projektového týmu Dodavatele a Objednatele. Projektový tým je skupina vybraných odborných pracovníků, kteří se účastní na Projektu a mají vyčleněné role a odpovědnosti.

V rámci Projektu jsou zastoupeny tyto orgány:

4.6.1.1. Řídící výbor (ŘV)

Představuje nejvyšší orgán Projektu, který akceptuje projektové výstupy, schvaluje změny, kontroluje a sleduje průběh Projektu. Je vrcholným rozhodovacím orgánem Projektu s primární úlohou udávat směr a zajišťovat rozhodování o Projektu.

ŘV rozhoduje na základě konsensu mezi Dodavatelem a Objednatelem. Hlavní rozhodovací zodpovědnost na straně Objednatele nese Ředitel projektu, jako osoba, která projekt řídí a je pověřená k činění právních úkonů ve vztahu k projektu a Sponzor projektu, jako předseda ŘV.

Řídící výbor projektu je odborným poradním orgánem ministra vnitra pro zajištění úspěšné přípravy a realizace projektu.

Řídící výbor projektu sjednocuje názory všech zainteresovaných stran, tj. zástupců Ministerstva vnitra ČR (dále jen MV ČR), Hasičského záchranného sboru ČR (HZS ČR) a Policie České republiky (PČR). Na jednání Řídícího výboru mohou být pozváni také zástupci Zdravotnické záchranné služby (ZZS). Členem Řídícího výboru projektu Dohledové centrum MV pro provoz ICT systémů a kybernetickou bezpečnost (SOCCR) je rovněž zástupce generálního dodavatele, České pošty s.p., Odštěpného závodu ICT služby.

Řídící výbor projektu zajišťuje efektivní komunikaci a spolupráci při realizaci projektu v rámci ministerstva vnitra, případně dalších orgánů státní správy.

Řídící výbor projektu projednává klíčové otázky a doporučuje řešení, která jsou následně schvalována ředitelem projektu, a to zejména:

- Strategické změny projektu;
- personální obsazení a podstatné změny rozsahu projektu;
- monitorování průběhu projektových prací;
- kontrola výstupů jednotlivých fází projektu a plánů pro fáze následující;
- ukončení projektu a rozpuštění vytvořené organizační struktury.

Řídícímu výboru projektu jsou eskalovány problémy a spory, které nebylo možné vyřešit na úrovni hlavního projektového týmu.

Složení ŘV

- Předsedou Řídícího výboru projektu je vrchní ředitel sekce provozu pro IKT.
- Členy Řídícího výboru projektu jsou Za stranu Objednatele:
 - Náместek ministra vnitra pro IKT
 - Ředitel projektu
 - Věcný gestor MVČR
 - Technický gestor MVČR



- Za stranu Dodavatele:
 - Člen ŘV – zástupce vedení dodavatele
 - Člen ŘV – zástupce dodavatele

Jednání ŘV se budou účastnit také PM za stranu Objednatele a PM za stranu Dodavatele, kteří budou pro jednání připravovat podklady ve formě Zprávy o stavu Projektu.

Členství v Řídícím výboru projektu je zastupitelné. Při neúčasti člena Řídícího výboru projektu jej může zastoupit jen jím pověřená osoba, která předkládá při jednání Řídícího výboru projektu písemné zmocnění k zastupování.

Členství v Řídícím výboru projektu zaniká:

- odvoláním;
- vzdáním se členství;
- úmrtím člena;
- ukončením služebního poměru příslušníka Policie České republiky nebo Hasičského záchranného sboru České republiky, případně pracovního poměru k ministerstvu vnitra.
- Předseda Řídícího výboru projektu může v době své nepřítomnosti zmocnit písemným pověřením jiného člena řídícího výboru projektu k svému zastupování při řízení jednání Řídícího výboru projektu.

Členové řídícího výboru projektu za Ministerstvo vnitra, Policii České republiky a Hasičský záchranný sbor České republiky jsou jmenováni a na základě návrhu předsedy řídícího výboru projektu odvoláváni ministrem vnitra.

Členové řídícího výboru projektu mají povinnost se zúčastnit jednání výboru. Nemohou-li se jednání zúčastnit, jsou povinni tuto skutečnost bez zbytečného odkladu oznámit předsedovi řídícího výboru projektu.

Pravomoci a odpovědnosti ŘV

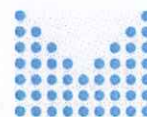
Pravomoci a odpovědnosti ŘV jsou následující:

- Přezkoumání a odsouhlasení navržené projektové dokumentace.
- Přezkoumávání a odsouhlasování projektových rizik, včetně plánu ošetření rizik.
- Schvalování a stanovování priorit nebo odložení žádostí o změny, které vyvstanou v průběhu Projektu a jsou předmětem změnového řízení.
- Odsouhlasení zásadních personálních změn v Projektu.
- Akceptace výstupů Projektu.
- Schválení ukončení Projektu.

ŘV se schází na začátku Projektu, při jednotlivých akceptacích včetně celkové finální akceptace celého dodávaného díla a v případě nutnosti také k řešení mimořádných situací.

Jednání ŘV svolává obvykle PM za stranu Objednatele, a to po dohodě s PM za stranu Dodavatele. V případě nutnosti řešit mimořádné situace pak může jednání ŘV svolat i kterýkoliv člen ŘV.

Z každého jednání ŘV je vypracován Dodavatelem Zápis, který je následně odsouhlasen všemi účastníky jednání a potvrzen podpisy jak zástupci Objednatele, tak Dodavatele.



Inicializace projektu

Projekt je inicializován prvním zasedáním Řídícího výboru a následně řízen prostřednictvím jednání jednotlivých týmů. Jednání týmů, kompetence a odpovědnosti v rámci týmů jsou popsány v této metodice.

První zasedání Řídícího výboru

Program prvního zasedání Řídícího výboru:

- Formální zahájení Projektu;
- v případě, že nejsou smlouvou dostatečně definovány oboustranně závazná pravidla řízení Projektu (role, odpovědnost), vzájemné komunikace a pravidla předání/převzetí plnění předmětu smlouvy, musí je stanovit ŘV v zápisu z 1. jednání.
- v případě, že nejsou smlouvou dostatečně definovány oboustranně závazné termíny nezbytné pro plnění projektu, je na ŘV ustanovit nebo aktualizovat harmonogram nebo Plán Projektu;
- stanovení/schválení závazných pravidel pro řízení Projektu;
- jmenování Hlavního projektového týmu dále též HPT (jmenovací listina, zápis ŘV či podepsaná Smlouva);
- stanovení/upřesnění harmonogramu řádných zasedání ŘV;
- stanovení termínu a místa příští schůzky ŘV a jejího předběžného programu;
- stanovení úkolů pro HTP;
- ostatní (zajištění komunikace, technické zázemí HTP, vstup do budov aj.);
- definování formy zápisu (vzor, struktura, písemně, elektronicky), okruh příjemců i forma distribuce a provedení dalších administrativních činností v závislosti na stanovených pravidlech řízení Projektu.

Mimořádné zasedání Řídícího výboru

Mimořádná schůzka ŘV se koná na podkladě vzniku mimořádné situace, která může vzniknout například jako neshoda stran v Hlavním projektovém týmu. Program mimořádného zasedání ŘV je následující:

- Řešení mimořádné situace, na podkladě které se schůzka koná;
- stanovení úkolů pro HPT;
- ostatní;
- sestavení zápisu a provedení dalších administrativních činností v závislosti na stanovených pravidlech řízení Projektu.

Poslední zasedání Řídícího výboru

Řádné zasedání ŘV se koná na podkladě schváleného harmonogramu a při příležitosti ukončení Projektu. Poslední zasedání ŘV má následující program:

- Převzetí vykonaného díla a uzavření Projektu;
- ukončení činnosti HPT a RT;

- ostatní;
- sestavení zápisu anebo předávacího protokolu a provedení dalších administrativních činností v závislosti na stanovených pravidlech řízení Projektu.

4.6.1.2. Hlavní projektový tým (HPT)

Představuje nejvyšší výkonný orgán Projektu. Má řídicí a rozhodovací pravomoci, v jejichž rámci provádí průběžné řízení Projektu a rozhoduje o postupu Projektu v mezích daných Smlouvou (příp. Plánem Projektu) a rozhodnutími ŘV.

V případě, že se nepodaří v rámci HPT dosáhnout dohody, je takový případ eskalován směrem k ŘV.

Složení HPT:

- Ředitel projektu za stranu Objednatele
- Vedoucí Projektu (PM) za stranu Objednatele
- Architekt řešení za Objednatele
- Vedoucí projektu (PM) za stranu Dodavatele
- Architekt řešení za Dodavatele
- Vedoucí odborných realizačních týmů Projektu

Pravomoci a odpovědnosti HPT:

- Řízení a kontrola postupu Projektu, vytváření operativního plánu.
- Dokumentování postupu Projektu (souladu i nesouladu).
- Vyhodnocování rizik Projektu a návrhy opatření na jejich eliminaci.
- Identifikace incidentů/problémů a návrhy opatření na jejich řešení.
- Monitoring práce jednotlivých modulových týmů a návrhy na změny ve složení týmů.
- Shromažďování a vyhodnocování změnových požadavků a zpracování návrhů na provedení změn.
- Vypracovávání pravidelných Zpráv o stavu Projektu pro HPT.

HPT se schází jednou týdně v průběhu celého Projektu. V případě potřeby se četnost schůzek bude operativně měnit s ohledem na aktuální stav a potřeby Projektu.

Schůzky HPT slouží primárně k projednávání aktuální situace na Projektu a plánování dalšího operativního postupu Projektu.

Schůzek HPT se účastní standardně jeho členové. Kromě nich se kdykoliv může zúčastnit i člen ŘV. Dále je možné přizvat na jednání další účastníky a to jak ze strany Dodavatele, tak ze strany Objednatele. V takovémto případě má PM, který další účastníky přizval, povinnost o tom ostatní účastníky informovat a stručně sdělit účel, proč byli na toto jednání přizváni.

Z každé schůzky HPT je vypracován Dodavatelem Zápis, který je na jednání schválen a stvrzen podpisy vedoucích Projektu.

Úkoly vyplývající z těchto schůzek jsou dále distribuovány na jednotlivé realizační týmy. Vedoucí Projektu za stranu Dodavatele a za stranu Objednatele předávají každý úkoly pouze v rámci vlastního projektového týmu.



První jednání Hlavního projektového týmu

První jednání HPT se koná na podkladě svolání schůzky ŘV. Program první schůzky HPT je:

- Zahájení činnosti;
- jmenování realizačních týmů dále též RT;
- stanovení/upřesnění harmonogramu řádných zasedání HPT;
- stanovení úkolů v závislosti na Plánu Projektu;
- stanovení úkolů termínů a odpovědností do příští schůzky HPT a přezkoumání podmínek pro plnění úkolů;
- stanovení termínu a místa příští schůzky HPT a jejího předběžného programu;
- stanovení úkolů pro RT;
- ostatní (zajištění komunikace, technické zázemí RT, vstup do budov aj.);
- definování formy zápisu (vzor, struktura, písemně, elektronicky), okruh příjemců i forma distribuce a provedení dalších administrativních činností v závislosti na stanovených pravidlech řízení Projektu.

4.6.1.3. Realizační týmy (RT)

Realizační týmy jsou pracovníci jednotlivých útvarů Objednatele, kteří zajišťují plnění jednotlivých dílčích úkolů Projektu. Realizační týmy na straně Dodavatele jsou odborné týmy zajišťující plnění dodávky.

V případě, že se nepodaří v rámci RT dosáhnout dohody, je takový případ eskalován směrem k HPT.

Složení RT:

- Zástupce Objednatele – Vedoucí RT;
- Zástupci Objednatele – klíčoví uživatelé;
- Zástupci Dodavatele – Vedoucí RT;
- Zástupci Dodavatele – odborné týmy;

RT jsou stanoveny na základě rozdělení dodávky s tím, že vyžádá-li si realizace dílčí části Projektu vznik nového týmu nebo změnu obsazení stávajícího, budou tyto změny projednány na HPT.

RT se scházejí na operativních schůzkách. Z každého jednání je vypracován Dodavatelem Zápis, který je po schválení všemi účastníky potvrzen podpisy jak zástupce Objednatele, tak Dodavatele.

Na jednání RT se standardně účastní členové RT. Kromě nich se může kdykoliv zúčastnit i člen HPT nebo člen ŘV. Dále je možné přizvat na jednání další účastníky a to jak ze strany Dodavatele, tak ze strany Objednatele. V takovémto případě má vedoucí RT povinnost informovat ostatní účastníky jednání o přizvaných osobách a stručně sdělit účel, proč byli na toto jednání přizváni.

Významnou roli v práci RT zastávají klíčoví uživatelé. Klíčový uživatel je podle pokynů vedoucího RT primárním zdrojem relevantních informací, potřebných pro správný postup realizace a je také primárně zodpovědný spolu s vedoucím RT za včasné otestování jednotlivých realizovaných kroků a přenášení poznatků na koncové uživatele, včetně zpracování uživatelských příruček.

Ustavující jednání realizačního týmu

První jednání RT se koná na podkladě svolání schůzky HPT. Program prvního jednání RT je následující:

- zahájení činnosti;
- stanovení/upřesnění harmonogramu řádných zasedání RT;
- stanovení úkolů do příští schůzky RT a přezkoumání podmínek pro plnění úkolů;
- stanovení termínu a místa příští schůzky RT a jejího předběžného programu;
- ostatní;
- definování zápisu a provedení dalších administrativních činností v závislosti na stanovených pravidlech řízení Projektu.

4.6.2. Role v rámci Projektu a jejich personální obsazení

- V rámci Projektu jsou jednotlivé osoby obsazovány do rolí. Role jsou definovány jak pro členy orgánů Projektu, tak pro členy realizačního týmu.
- Níže je uveden podrobný popis jednotlivých rolí, které budou tyto role plnit v rámci tohoto Projektu.
- V této Metodice jsou vyjmenovány hlavní role standardně se vyskytující v rámci Projektů a popis jejich typických činností.
- Je reprezentován některým z klíčových představitelů Objednatele, který má dostatečné rozhodovací pravomoci ohledně způsobu řízení Projektu. Sponzor Projektu je obvykle předsedou ŘV Projektu.
- Mezi hlavní úkoly **Sponzora Projektu** patří např. následující aktivity:
- Oficiální zaštitění celého projektu v rámci organizace.
- Návrh a realizace strategických rozhodnutí, která mají vliv na směřování projektu.
- Rozhodování sporných případů předaných ŘV k vyřešení.
- Zajišťování nezbytné podpory Projektu ze strany vedoucích složek Objednatele.
- Rozšiřování povědomí o Projektu na straně Objednatele (včetně přímo nezúčastněných složek).
- Další aktivity, které souvisejí s působností ŘV.

4.6.2.1. Role Dodavatele:

Ředitel programu

Je osobou oprávněnou činit veškerá rozhodnutí a právní úkony v rámci projektu a předmětu smlouvy.

Mezi hlavní úkoly Ředitele projektu patří:

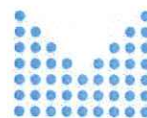
- návrh jmenování Projektového manažera a ustavení jeho pravomocí a odpovědností;
- definování věcných cílů projektu na globální i detailní úrovni;
- Vytvoření podmínek pro sladění projektu s dalšími aktivitami organizace.
- Autorizace výdajů organizace.



- Kontrolu postupu projektu ze strategického hlediska.
- Rozhodnutí o oficiálním zahájení a ukončení etap projektu.
- Řízení a kontrola projektu jako celku.
- Kontrola efektivity řízení rizik.
- Provedení kontroly dopadů potenciálních změn na cíle projektu.
- Výběr Dodavatele a uzavření smlouvy s Dodavatelem.
- Informování Sponzora projektu o stavu projektu.
- Organizace a řízení jednání Hlavního projektového týmu.
- Eskalace problémů strategické povahy na Řídící výbor projektu.
- udržování kvalitní výměny informací s resortní PMO;
- schvalování projektových standardů;
- předložení návrhů na provedení změn, které byly projednány, analyzovány a doporučeny Hlavním projektovým týmem, Radě pro koordinaci u strategického projektu, event. Řídícímu výboru u standardního projektu.

Projektový manažer

- Povede Projekt na straně Dodavatele a jako takový řídí každodenní aktivity na Projektu v koordinaci s vedoucím Projektu na straně Dodavatele.
- Vedoucí Projektu vykonává zejména následující činnosti:
- Prověřuje skutečnosti vedoucí k naplnění cílů Projektu, tvoří strategii Projektu a řídí celý Projekt na straně Dodavatele.
- Zajišťuje a koordinuje požadované zdroje Projektu ze strany Dodavatele (je-li výslovně dohodnuto, může i koordinovat zdroje na straně Objednatele), a to v požadované kapacitě, kvalitě a množství podle platného harmonogramu.
- Kontroluje dodržování projektového postupu a harmonogramu.
- Řeší běžné problémy související s Projektem na straně Dodavatele.
- Vede dokumentaci a dohlíží na straně Dodavatele na dodržování všech projektových postupů a procedur definovaných a schválených v rámci Plánu projektu.
- Odpovídá za dodržování schváleného rozpočtu;
- Odpovídá za řízení dodávek a všech dalších Dodavatelem poskytovaných služeb.
- Odpovídá za proces plánování a řízení rizik Projektu na straně Dodavatele.
- Odpovídá za kvalitu výstupů (dokumentů), které jsou v rámci poskytovaných služeb vytvářeny.
- Odpovídá za bezpečnost informací v rámci Projektu.
- Odpovídá za vypracovávání pravidelných Zpráv o stavu projektu ŘV.
- Odpovídá za koordinaci činností Dodavatele vzhledem k organizaci a lidským zdrojům organizace, v součinnosti s Projektovým manažerem
- V případě nezbytnosti navrhuje změny v projektovém týmu Dodavatele.



- Vedoucí Projektu za Dodavatele je vedoucím členem vedení Projektu na straně Dodavatele a odpovídá ŘV Projektu.
- Tato role je v dokumentaci k Projektu též užívána pod názvem Vedoucí Projektu za Dodavatele.

Zástupce projektového manažera

Podporuje v činnosti Projektového manažera, v jeho nepřítomnosti ho zastupuje.

Zástupce projektového manažera se podílí na následujících činnostech:

- Prověřuje skutečnosti vedoucí k naplnění cílů Projektu, tvoří strategii Projektu a řídí celý Projekt na straně Dodavatele;
- Zajišťuje a koordinuje požadované zdroje Projektu ze strany Dodavatele (je-li výslovně dohodnuto, může i koordinovat zdroje na straně Objednatele), a to v požadované kapacitě, kvalitě a množství podle platného harmonogramu;
- Kontroluje dodržování projektového postupu a harmonogramu;
- Řeší běžné problémy související s Projektem na straně Dodavatele;
- Vede dokumentaci a dohlíží na straně Dodavatele na dodržování všech projektových postupů a procedur definovaných a schválených v rámci Plánu projektu;
- Odpovídá za dodržování schváleného rozpočtu;
- Odpovídá za řízení dodávek a všech dalších Dodavatelem poskytovaných služeb;
- Odpovídá za proces plánování a řízení rizik Projektu na straně Dodavatele;
- Odpovídá za kvalitu výstupů (dokumentů), které jsou v rámci poskytovaných služeb vytvářeny;
- Odpovídá za bezpečnost informací v rámci Projektu;
- Odpovídá za vypracovávání pravidelných Zpráv o stavu projektu ŘV;
- Odpovídá za koordinaci činností Dodavatele vzhledem k organizaci a lidským zdrojům organizace, v součinnosti s Projektovým manažerem;
- V případě nezbytnosti navrhuje změny v projektovém týmu Dodavatele.

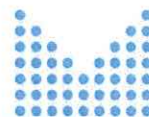
Solution Architect

Tato pozice bude obsazena odborníkem s patřičnými zkušenostmi a znalostmi, který bude plně odpovědný za dvě oblasti Projektu:

- Vytvoření návrhu celkové architektury Projektu.
- Prosazení navržené architektury.

V souvislosti s výše uvedeným bude hlavní technický architekt provádět v rámci projektu následující aktivity:

- Odborné řízení a koordinace týmu architektů po celou dobu jejich působení na Projektu.
- Spolupráce s technickým týmem při zpracování Návrhu architektury řešení, Inženýringu a Technického projektu.
- Spolupráce s Bezpečnostním manažerem při návrhu bezpečnostní architektury řešení.



- Spolupráce s pracovníky Objednatele, za účelem zpracování standardů architektury a
- Zodpovědnost (reportování) vedoucímu projektu za Dodavatele.
- Solution architekt bude členem vedení projektu na straně Dodavatele.

Síťový architekt

Tato pozice bude obsazena odborníkem s patřičnými zkušenostmi a znalostmi, který bude odpovědný za oblasti Projektu:

- samostatné provádění prací či práce v projektovém týmu na externích či interních projektech v klíčové roli specialisty zodpovědného za návrh architektury sítí a systémového IT řešení dle specifikace zákazníka
- plnění role specialisty nebo odborného garanta, provádění návrhu architektury „High level“ nebo komplexního IS složeného typicky z několika systémů a integrační platformy
- komunikace návrhů se Solution Architektem
- zodpovědnost za správnost, efektivnost a spolehlivost navrženého řešení či integrační architektury
- provádění analýz a návrhů HW architektury (sizing a umístění HW, zejména servery, pole, archivace, zálohování, klientské stanice a další HW komponenty, které nemají čistě síťový charakter)

Administrátor projektu

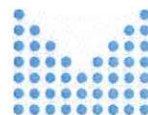
Bude asistovat Vedoucímu Projektu na straně Dodavatele a pod jeho vedením zajišťovat zejména administrativní úkony spojené s řízením Projektu.

Asistent/Administrátor Projektu bude podřízen Vedoucímu Projektu na straně Dodavatele.

Bezpečnostní manažer

Tato pozice bude obsazena odborníkem s patřičnými zkušenostmi a znalostmi, který bude odpovědný za oblasti Projektu:

- odpovědnost za informační bezpečnost projektu během celého životního cyklu projektu a za informační bezpečnost
- sledování změn legislativy a vyhodnocování jejich vlivu na informační bezpečnost
- Dále bude zajišťovat:
- Zpracování bezpečnostního projektu pro projekt;
- Zpracování návrhu systémové bezpečnostní politiky;
- Zpracování návrhu řešení správy uživatelů;
- Prosazení navržené koncepce a specifikace;
- Zpracování další bezpečnostní dokumentace k vytvořenému projektu
- Nasazení přiměřených ochranných opatření pro zajištění bezpečnosti informací v rámci Projektu;
- Dohled nad implementací a testováním navržených bezpečnostních opatření.



Bezpečnostní manažer Projektu bude členem vedení projektu na straně Dodavatele.

Konfigurátor

Tato pozice bude obsazena odborníkem s patřičnými zkušenostmi a znalostmi, který bude odpovědný za oblasti Projektu:

- Vytvoření konfiguračních plánů sítě dle prováděcího projektu
- Realizace konfigurace parametrů jednotlivých zařízení
- Provádění FAT testů ve spolupráci se Sítovými architekty

Implementátor

Tato pozice bude obsazena odborníkem s patřičnými zkušenostmi a znalostmi, který bude odpovědný za oblasti Projektu:

- Spolupráce na tvorbě prováděcích projektů, analýza stávající situace a spolupráce s architekty na finálním stavu
- Implementace zařízení na určených síťových lokalitách
- Provádění SAT testů ve spolupráci se Sítovými architekty

Konzultant sekce KI

Tato pozice bude obsazena odborníkem s patřičnými zkušenostmi a znalostmi, který bude odpovědný za oblasti Projektu:

- Samostatné provádění prací či práce v projektovém týmu na externích či interních projektech v klíčové roli specialisty zodpovědného za návrh architektury sítí a systémového IT řešení s ohledem na budoucí provoz.
- Plnění role specialisty nebo odborného garanta
- Komunikace návrhů se Solution Architektem
- Zodpovědnost za správnost, efektivnost a spolehlivost navrženého řešení či integrační architektury z pohledu budoucího provozu.

Dokumentarista

Tato pozice bude obsazena odborníkem s patřičnými zkušenostmi a znalostmi, který bude odpovědný za oblasti Projektu:

- Kontrola formální správnosti dokumentace
- Finální úpravy výstupů

Právník

Tato pozice bude obsazena odborníkem s patřičnými zkušenostmi a znalostmi, který bude odpovědný za oblasti Projektu:

- Zajišťování právní agendy spojené s projektem
- Zpracování právních stanovisek a poskytování konzultací k právním
- Komunikace s externími právními poradci

Konzultant

Tato pozice bude obsazena odborníkem s patřičnými zkušenostmi a znalostmi, který bude odpovědný za oblasti Projektu:

- Identifikuje možnosti zlepšování realizace a provozu
- Posuzuje jejich proveditelnost
- Koordinuje rozvojové a návrhové činnosti
- Provádí odborný dohled nad implementačními pracemi
- Zajišťuje rozbor a analýzy návrhů architektury řešení
- Samostatná práce nebo práce člena projektového týmu dle zadání
- Podíl na zpracování přípravě a zpracování projektu
- Monitoring a koordinace projektů ve svěřené oblasti

Specialista nákupu

Tato role participuje na akvizičních procesech dle Zákona č. 137/2006 Sb., o veřejných zakázkách pro zajištění nezbytných služeb, technického zařízení a souvisejících prostředků v rámci projektu.

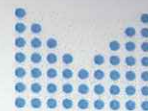
Tato pozice bude obsazena odborníkem s patřičnými zkušenostmi a znalostmi, který bude odpovědný za oblasti Projektu:

- Příprava podkladů pro zahájení nákupního procesu, spolupráce při tvorbě zadávací dokumentace.
- Správa komodit s cílem standardizace a unifikace nakupovaných položek a optimalizace portfolia dodavatelů.
- Činnosti spojené s vyhodnocování nákupního procesu.
- Zpracování analýz procesů, stavu rizikových oblastí.

4.6.2.2. Role Objednatele:**Ředitel projektu**

Ředitel projektu zejména zodpovídá za:

- návrh jmenování Projektového manažera a ustavení jeho pravomocí a odpovědností;
- definování věcných cílů projektu na globální i detailní úrovni;
- vytvoření podmínek pro sladění plánu projektu s dalšími aktivitami organizace;
- autorizaci výdajů organizace;
- kontrolu postupu projektu ze strategického hlediska (soulad se Zadávací dokumentací projektu);
- rozhodnutí o oficiálním zahájení a ukončení fází projektu;
- řízení a kontrolu projektu jako celku;
- kontrolu efektivity řízení rizik;



- provedení kontroly dopadů potenciálních změn na cíle projektu;
- výběr Dodavatele a uzavření smlouvy s Dodavatelem;
- informování Sponzora projektu o stavu projektu;
- organizaci a řízení jednání Hlavního projektového týmu;
- eskalaci problémů strategické povahy na nadřízenou složku (Řídící výbor projektu);
- udržování kvalitní výměny informací s resortní PMO;
- schvalování projektových standardů;
- předložení návrhů na provedení změn, které byly projednány, analyzovány a doporučeny Hlavním projektovým týmem, Radě pro koordinaci u strategického projektu, event. Řídícímu výboru u standardního projektu.

Projektový manažer

- Projektový manažer vede Projekt na straně Objednatele a odpovídá za zajištění interních zdrojů a kapacit a jejich koordinaci s Dodavatelem ve společných týmech pracujících na jednotlivých výstupech.
- Projektový manažer provádí zejména následující činnosti:
- Řídí a organizuje práci projektového týmu. Pravomoc a odpovědnost projektového manažera je odvozena z pravomoci a odpovědnosti Ředitele projektu a jím vymezena se zřetelem k úkolům projektového týmu;
- Podílí se na přípravě složení projektového týmu, nastavení odpovědnosti projektového týmu a kompetencí členů projektového týmu, zpracování pracovní náplně jednotlivých členů a povinností členů projektového týmu;
- Stanoví formy a způsoby realizace úkolů, jejichž plnění přísluší jím řízenému projektovému týmu;
- Zajišťuje pro Projekt požadované interní zdroje v požadované kapacitě, kvalitě a množství podle platného harmonogramu.
- je v rámci vymezených povinností, pravomocí a odpovědností povinen zajistit fungování vnitřního kontrolního systému;
- Řeší běžné problémy související s Projektem.
- Vede dokumentaci a dohlíží na dodržování projektových postupů a procedur definovaných a schválených v rámci Plánu Projektu.
- Odpovídá za úplnost podkladů pro Změnová řízení.
- Rozhoduje o závažnosti problémů a jejich eskalaci na ŘV a iniciuje vlastní hlášení problémů vůči ŘV.
- je v rámci vymezených povinností, pravomocí a odpovědností povinen zajistit fungování vnitřního kontrolního systému;
- spravuje a aktualizuje údaje projektu v projektovém informačním systému
- Navrhuje a schvaluje nezbytné změny v projektovém týmu Objednatele.
- Projektový manažer na straně Objednatele zodpovídá ŘV Projektu.



Věcný gestor projektu

Je zástupcem na straně Objednatele. Věcný gestor projektu bude koordinovat soulad věcného obsahu projektu a technických požadavků ZoKB a požadavků systémů CMS 2.0, NIS IZS, ITS NGN a KSP a bude zastupovat projekt v řídicích strukturách tohoto a dalších relevantních projektů MV ČR.

- Je zodpovědný za přesnou specifikaci výstupů projektu;
- V průběhu projektu je pověřen kontrolou konzistence dosavadních výsledků směrem k cíli projektu;
- Má zodpovědnost za správnost předmětu objednávek a smluv s dodavateli po věcné stránce;
- Propaguje výstupy projektu;
- Zajišťuje alokaci času koncových uživatelů;
- Garantuje soulad produktu projektu s požadavky uživatelů a naplnění očekávaných přínosů pro uživatele.

Věcný gestor projektu má na starosti dohled nad technickou stránkou projektu; komunikaci s ostatními zainteresovanými stranami při investicích do údržby, oprav HW a upgrade SW.

Technický gestor projektu

Je zástupcem na straně Objednatele. Technický gestor podporuje Projektového manažera a Věcného gestora projektu.

Úlohou technického gestora je zejména:

- podpora Projektového manažera a Věcného gestora projektu při správném výběru pracovníků, případně při úpravách projektové organizace;
- kompatibilita technické stránky řešení s používanými technologiemi organizace;
- průzkum technických a technologických procedur, zajištění jejich adekvátnosti a efektivnosti, identifikace a přijímání nezbytné korektivní akce (vystane-li její potřeba);
- navržení základního řešení projektu a záruka, že odpovídá cílům projektu;
- vznik a trvalá údržba konzistentního, moderního a dostatečně technologicky robustního řešení projektu (na jeho nízkých technologických vrstvách až po síťovou vrstvu včetně);
- odpovídá za technickou správnost a proveditelnost řešení;
- jednoznačnost a technická správnost předmětu smlouvy s Dodavatelem;
- oponentura a schválení řešení všech dodavatelských firem;
- průběžná kontrola kvality dílčích výstupů projektu (eskalace zjištěných nedostatků na úroveň Hlavního projektového týmu);
- identifikace technických a technologických problémů a neshod, iniciace procedur řízeného řešení problémů (eskalace na Ředitele projektu);
- koordinace činností Řešitelských týmů v technicko-technologické oblasti při řešení interdisciplinárních neshod (rozporovací řízení při řešení sporů);
- zajišťuje a kontroluje soulad zadání Objednatele s výstupy Dodavatele

Administrátor projektu

Administrátor projektu především:

- administrativně podporuje týmy projektu;
- distribuuje zápisy a podklady zúčastněným osobám;
- poskytuje odpovídající informace relevantním osobám;
- organizuje schůzky podle existujících plánů projektu a pokynů Ředitele projektu;
- sleduje a požaduje plnění plánovaných i operativních administrativních úkonů vyplývajících z plánu řízení projektu a ze zápisů z jednání;
- vede dokumentaci projektu;
- zajišťuje a kontroluje, zda jsou dodržovány postupy práce s formalizovanými dokumenty
- a zda jsou správně užívány všechny formuláře a standardy (k tomuto účelu zajišťuje
- nezbytné instruktáže a školení);
- odpovídá za správné vyplnění, pojmenování a uložení všech standardních formulářů, které jsou používány v projektu, jakož i všech dokumentů, které jsou ukládány v projektové knihovně (ukládat dokumenty do projektové knihovny je oprávněn výlučně Administrátor projektu, vyzvedávat a používat dokumenty z projektové knihovny mohou všichni pracovníci projektového týmu);
- administruje a řídí jednotlivé verze dokumentů - distribuuje aktuální znění dokumentů relevantním osobám.

4.6.3. Komunikační matice

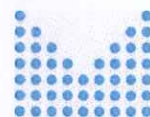
Komunikační matice je dokument obsahující kontaktní informace o všech relevantních osobách na straně Objednatele a Dodavatele. V průběhu celého Projektu bude Komunikační matice průběžně aktualizována a její aktuální verze bude k dispozici všem členům projektového týmu jako součást sady projektových dokumentů.

4.6.4. Odpovědnosti včetně podpisových práv

Za provedení prací v jednotlivých fázích Projektu jsou zodpovědní vedoucí příslušných Realizačních týmů. PM za Objednatele a PM za Dodavatele jsou odpovědní za včasné a úplné dodání Díla.

Podpisová práva k jednotlivým dokumentům vystavovaným v rámci Projektu jsou nastavena takto:

Dokument	Podpisové právo za Objednatele	Podpisové právo za Dodavatele
Plán Projektu	Ředitel projektu	Sponzor ŘV / Člen ŘV
Předávací Protokol	PM (převzetí díla nebo jeho části)	PM (předání díla nebo jeho části)
Akceptační Protokol	Ředitel projektu	Sponzor ŘV / Člen ŘV
Zápis z jednání ŘV	Předseda ŘV / Ředitel projektu	Sponzor ŘV / Člen ŘV
Zápis z jednání HTP	PM	PM
Zápis z jednání RT	Vedoucí RT / PM	Vedoucí RT / PM



Zpráva o stavu Projektu	Vedoucí RT / PM	Vedoucí RT / PM
Změnový požadavek	Ředitel projektu	Sponzor ŘV / Člen ŘV

4.6.5. Eskalační procedura

Cílem eskalační procedury je řešení eskalovaných problémů nevyjasněných záležitostí a rizik na vrcholové úrovni řízení projektu v rámci Řídícího výboru projektu.

4.6.6. Dokumenty vedené v Projektu

V rámci Projektu se vystavují dokumenty, které slouží jednak k vlastnímu řízení Projektu a jednak k formalizaci a odsouhlasení jednotlivých výstupů Projektu.

Dokumenty budou zpracovány do 20. 1. 2015 a budou schváleny dle Odpovědnosti 7.4. Odsouhlasené vzory dokumentů vedených v Projektu se stanou nedílnou součástí této Metodiky.

Sada těchto dokumentů zahrnuje:

- **Zpráva o stavu Projektu**

Formální pravidelná zpráva o stavu Části (etapy) Projektu, kterou projektový manažer Dodavatele předkládá Objednateli. Obvykle je vystavován v pravidelných, nejčastěji měsíčních periodách.

- **Plán Projektu**

Dokument definující nastavení, účel, pravidla a způsob provádění Projektu. Za jeho vypracování a průběžnou aktualizaci odpovídají společně PM za Dodavatele a PM za Objednatele. Všechny aktualizace musí být schváleny Řídícím výborem.

- **Registr Rizik**

Dokument obsahující soupis aktuálních rizik identifikovaných na Projektu a plán jejich eliminace i postupu pro případ, že přes veškerá provedená opatření nastanou.

- **Issue Log**

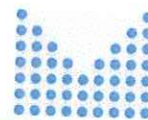
Dokument obsahující soupis požadavků (předmětu Díla), otevřených problémů, incidentů, změnových požadavků a dalších otevřených situací na Projektu včetně evidence jejich aktuálního stavu zejména s ohledem na stav dodání, akceptace, vad, dodání dokumentace, provedení školení a odkazu na dokumentaci s jejich popisem nebo protokoly.

- **Komunikační matice**

Dokument obsahující kompletní kontaktní informace o všech osobách spojených s Projektem, na straně Objednatele, Dodavatele.

- **Zpráva o stavu Projektu pro HPT**

Dokument poskytující přehled o aktuálním stavu Projektu, včetně soupisu rizik a otevřených bodů, příp. i změn. Je aktualizována PM za Dodavatele a předávána jako podklad pro pravidelné schůzky HPT.



- **Zápis z jednání/schůzky**

Záznam pořizovaný Dodavatelem z každého jednání/schůzky, které v rámci Projektu proběhne (jednání ŘV, jednání HPT, jednání RT atd.). Tento dokument obvykle obsahuje následující náležitosti:

- seznam všech účastníků jednání
- obsah jednání
- rozbor splnění úkolů z předešlého jednání (schůzky)
- úkoly na další období
- požadavky na rozhodnutí ŘV, pokud se vyskytnou
- termín konání dalšího jednání

Mimo úkolů jsou obvykle součástí zápisu i další doplňující informace, které vedou k objasnění činností vykonávaných v rámci Projektu nebo informace, které blíže upřesňují stav určitých činností (úkolů).

Zápisy provádějí a za obsah odpovídají společně PM za Objednatele a PM za Dodavatele (nebo jimi pověřené osoby, pokud se PM schůzek neúčastní). Za Zápisy ze schůzek RT odpovídají vedoucí RT (nebo jimi pověřené osoby).

Každý zápis je distribuován účastníkům jednání/schůzky do tří pracovních dnů od uskutečnění jednání/schůzky. Za rozeslání zápisu odpovídá vedoucí Projektu za Dodavatele. Přípomínky k zápisu je třeba uplatnit u PM nejpozději dva následující pracovní dny po jeho obdržení.

- **Předávací Protokol**

Formulář, kterým předává Dodavatel dílčí plnění nebo celý předmět plnění po jeho ukončení Objednateli a Objednatel jej za podmínek stanovených Smlouvou přebírá.

- **Akceptační Protokol**

Protokol potvrzující, že Dodavatel řádně splnil své závazky vyplývající ze Smlouvy a Objednatel takové Dílo akceptoval.

4.7. Akceptace

4.7.1. Typy akceptací

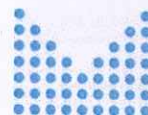
Smluvní strany se dohodly na následujících typech akceptací:

- **Dílčí akceptace:**

Předmětem dílčích akceptací je posouzení kvality výstupů jednotlivých částí Díla a jejich souladu s vymezením předmětu Díla ve Smlouvě.

- **Doplňkové akceptace:**

Předmětem doplňkových akceptací jsou doplňující ověření částí Díla v rámci změnového řízení či jejich vzájemného souladu (např. doplňkové integrační testy). Doplňkové akceptace mohou být prováděny na základě dohody Hlavního projektového týmu a schválení ŘV.



- **Celková akceptace:**

Předmětem celkové akceptace je ověření splnění hlavních milníků provádění Díla a splnění Smlouvy. Celková akceptace je typově obdobná v následujícím bodě uvedené závěrečné akceptaci (užívá se závěrečný akceptační protokol). Celkové akceptaci podléhá každá část (milník) časového harmonogramu plnění provádění Díla.

- **Závěrečná akceptace:**

Předmětem závěrečné akceptace je celkové ověření splnění závazku provést Dílo a splnění Smlouvy. K závěrečné akceptaci může být Dílo připuštěno, pouze pokud celková akceptace Etap/částí je ukončena s výsledkem „Akceptováno“.

4.7.2. Akceptační kritéria

Akceptační kritéria musí být plně v souladu se závaznou Specifikací Předmětu plnění (Technický projektem). Specifikace Předmětu plnění musí definovat požadované vlastnosti výstupů. Jedná se zejména o specifikaci požadovaných funkčních a kvalitativních parametrů předmětu plnění a stanovení způsobu jejich ověření. Akceptační kritéria jsou v rámci projektu stanovena na čtyřech základních úrovních:

- **Rámcová akceptační kritéria:**

Rámcová akceptační kritéria jsou dána dikcí Specifikace Předmětu plnění, která definuje vlastnosti Díla. Ověřuje-li se formou akceptace vymezená část Díla, pak musí splňovat veškeré specifikace a požadavky uvedené ve Specifikaci Předmětu plnění (rámcová akceptační kritéria).

- **Dílčí akceptační kritéria:**

Dílčí akceptační kritéria se vztahují na předloženou část Díla vymezenou k dílčí akceptaci, včetně zohlednění vývoje její specifikace v průběhu její realizace, stanoví jednoznačný způsob, postupy a podmínky jejího ověřování, včetně návrhu časového harmonogramu akceptačního řízení podle těchto kritérií tak, aby jejich schválením obě strany odsouhlasily i dobu a délku potřebnou k provedení akceptačního řízení. Ověřuje-li se formou akceptace vymezená část Díla, pak musí splňovat veškeré specifikace a požadavky uvedené ve Specifikaci Předmětu plnění.

- **Celková akceptační kritéria:**

Celková akceptační kritéria se vztahují na předloženou část Díla vymezenou k celkové akceptaci, včetně zohlednění vývoje její specifikace v průběhu její realizace, stanoví jednoznačný způsob, postupy a podmínky jejího ověřování, včetně návrhu časového harmonogramu akceptačního řízení podle těchto kritérií tak, aby jejich schválením obě strany odsouhlasily i dobu a délku potřebnou k provedení akceptačního řízení.

- **Závěrečná akceptační kritéria:**

Závěrečná akceptační kritéria jsou formálním ověřením výsledků a závěrů celkových akceptací.

4.7.3. Akceptační procedura

Akceptační proces je definován za účelem předání a převzetí Díla (nebo dílčího plnění), které bylo dokončeno. Výrok pro akceptaci Díla (nebo dílčího plnění) může být následující:

- a) Akceptováno bez výhrad (tj. bez vad a nedodělků)
nebo
- b) Akceptováno s výhradami, které však nebrání převzetí díla nebo jeho části ze strany Objednatele.
- c) Neakceptováno

Za úspěšnou akceptaci se považuje písemná akceptace s výrokem Akceptováno.

Dosažení úspěšné písemné akceptace je podmínkou finančního plnění jednotlivých fakturačních milníků.

Akceptace probíhá vždy v souladu s definovanými akceptačními kritérii a její výsledek je zaznamenán v Akceptačním protokolu, který je postoupen ke schválení ŘV. Součástí Akceptačního protokolu je také seznam osob Objednatele, které mají oprávnění hlásit případné problémy či vady dílčího plnění a seznam kontaktních osob Dodavatele odpovědných za jejich řešení.

Akceptační proces může být realizován pouze osobami s patřičnými podpisovými pravomocemi v rámci organizace Projektu, viz kapitola Odpovědnosti včetně podpisových práv.

Předmětem řádného předání a převzetí je také příslušná technická, provozní a jiná dokumentace vztahující se k plnění nebo jeho části, pokud existuje.

Podmínky Akceptace díla nebo dílčího plnění, podmínky Předložení Akceptačního protokolu k podpisu, Akceptační kritéria, Seznam akceptačních kritérií, Klasifikace vad a nedodělků pro předání díla či dílčího plnění budou detailně definovány a schváleny ŘV.

4.7.4. Klasifikace vad a nedodělků pro předání díla či dílčího plnění

Vadou se rozumí nesoulad funkcionality Díla nebo dílčího plnění s funkcionalitou definovanou ve Specifikaci Předmětu plnění nebo ovlivnění spolupracujících systémů takovým způsobem, že jsou kritickým způsobem ovlivněny hlavní činnosti Objednatele.

Kategorie	Vada	Popis
A	Kritická	Jedná se o vadu Díla nebo jeho části, která je v přímém rozporu se zadáním Objednatele, brání přechodu k další části plnění nebo kvalitou či kvantitou hrubě neodpovídá požadované úrovni nebo rozsahu. Může se jednat např. o chybějící či zcela nedostatečný výstup, zásadní chybu v návrhu či posouzení, zcela nevhodně zvolený postup, který je v přímém rozporu s technickou či ekonomickou relevancí vůči zadání, nebo tyto vady způsobí, že některé nebo všechny systémy podporující hlavní procesy selhaly a jsou zcela nefunkční nebo je jejich funkčnost omezena tak, že je kritickým způsobem ovlivněna činnost Objednatele. Z důvodu vady Díla (dílčího plnění) některé nebo všechny systémy

		podporující hlavní procesy selhaly a jsou zcela nefunkční nebo je jejich funkčnost omezena tak, že je kritickým způsobem ovlivněna činnost Objednatele.
B	Vážná	Jedná se o vadu Díla nebo jeho části, která má charakter nedostatečného, chybného nebo chybějícího výstupu dle zadání a kvalitativně tak neodpovídá požadavkům Objednatele. Může se jednat např. o vadu výstupu, která by měla za následek ovlivnění funkčního celku, chybějící část některého z celků plnění nebo by touto vadou došlo k výraznému ovlivnění činnosti Objednatele z důvodu selhání nebo omezení některé ze systémových funkcí podporujících důležité procesy. Z důvodu vady Díla (dílčího plnění) je činnost Objednatele výrazně ovlivněna z důvodu selhání nebo omezení některé ze systémových funkcí podporujících důležité procesy. Tato vada znemožňuje nebo výrazně komplikuje využívání systému Díla (dílčí plnění).
C	Drobná	Jedná se o nedostatky, které nepředstavují překážky z hlediska formy, relevance obsahu či technického řešení vlastního Předmětu plnění nebo jeho části a nemají tak zásadní vliv na kvalitu Díla nebo jeho části Tato kategorie zahrnuje funkce, které sice zcela selhaly, ale nejsou v daný moment využívány a nemají žádný vliv na řádný chod systému. Vada má zanedbatelný vliv na činnost Objednatele. Vada se vyskytuje v izolované části Díla (dílčího plnění) – využívání Díla (dílčího plnění) je částečně ztíženo a nemá vliv na ostatní funkce.
D	Kosmetická	Dílo nebo jeho část je plně funkční, vada je pouze kosmetického charakteru. Tato vada nemá vliv na činnost Objednatele. Vada nekomplikuje využívání Díla nebo jeho části.

Kategorizaci vad provádí Vedoucí projektu Objednatele s následným potvrzením Vedoucím projektu Dodavatele s cílem dosáhnout shody v kategorizaci vad.

V případě neshody Vedoucích projektu v kategorizaci vad toto musí být uvedeno v akceptačním protokolu a je povinností Vedoucího projektu (PM) Dodavatele svolat mimořádný Řídicí výbor tak, aby bylo Řídicím výborem projektu rozhodnuto o kategorizaci vady, a to do termínu nejbližšího předání předmětu celkové akceptace k akceptaci, v rámci které je rozporovaná vada součástí.

4.7.5. Výsledky akceptačního řízení

Definice výsledků dílčích akceptací

Smluvní strany se dohodly na následující definici výsledků dílčích akceptací:

- Akceptováno - Pro výrok a formulaci dílčího akceptačního rozhodnutí Akceptováno je podmínkou úspěšné odstranění všech vad kategorie A i B uvedených a platných v průběžném akceptačním protokolu.
- Akceptováno s výhradou - Pro výrok a formulaci dílčího akceptačního rozhodnutí Akceptováno s výhradou je podmínkou úspěšné odstranění všech vad kategorie A uvedených a platných v průběžném akceptačním protokolu.
- Neakceptováno - Pro výrok a formulaci dílčího akceptačního rozhodnutí Neakceptováno je podmínkou neúspěšné odstranění vad kategorie A uvedených a platných v průběžném akceptačním protokolu.

Definice výsledků celkové akceptace

- Akceptováno - Pro výrok a formulaci celkového akceptačního rozhodnutí Akceptováno je podmínkou úspěšné ukončení všech dílčích akceptací dané etapy dle harmonogramu plnění předmětu akceptace a to jen ve stavu Akceptováno. Musí být odstraněny veškeré vady A (kritická vada) i B (vážná vada), vad kategorie C (drobná vada) formulované v akceptačních protokolech a zůstává neodstraněných maximálně patnáct (15) vad kategorie D (kosmetická vada). K těm navrhne Dodavatel termín a harmonogram odstranění.
- Akceptováno s výhradou - Pro výrok a formulaci celkového akceptačního rozhodnutí Akceptováno s výhradou je podmínkou úspěšné ukončení všech dílčích akceptací dané etapy dle harmonogramu plnění předmětu akceptace. Musí být odstraněny veškeré vady kategorie A (kritická vada), může zůstat maximálně pět (5) vad kategorie B (vážná vada), maximálně deset (10) vad kategorie C (drobná vada) a maximálně patnáct (15) vad kategorie D (kosmetická vada). K těm navrhne Dodavatel termín a harmonogram odstranění.
- Neakceptováno - Pro výrok a formulaci celkového akceptačního rozhodnutí Neakceptováno je podmínkou neúspěšné ukončení (nedokončení) kterékoliv z dílčích akceptací dané etapy dle harmonogramu plnění předmětu akceptace a/nebo neodstranění jakékoliv vady kategorie A (kritická vada) a/nebo existence více jak pěti (5) vad kategorie B (vážná vada) a/nebo existence více než deseti (10) vad kategorie C (drobná vada) a více jak patnácti (15) vad kategorie D (kosmetická vada).

Definice výsledků závěrečné akceptace

- **Akceptováno** - Pro řádné splnění Smlouvy, kterým je výrok a formulace závěrečného akceptačního rozhodnutí Akceptováno je podmínkou úspěšné odstranění všech vad/incidentů kategorie A (kritická vada) i B (vážná vada) a zůstává neodstraněných nejvýše pět (5) vad/incidentů kategorie C (drobná vada) nebo deset (10) vad/incidentů kategorie D (kosmetická vada). K těm navrhne Dodavatele termín a harmonogram odstranění.
- **Neakceptováno** - Pro výrok a formulaci závěrečného akceptačního rozhodnutí Neakceptováno je podmínkou neúspěšné odstranění jakékoliv vady/incidentu kategorie A nebo B a/nebo existence neodstraněných více jak pět (5) vad/incidentů kategorie C a existence neodstraněných více jak deset (10) vad/incidentů kategorie D (kosmetická vada).
Postup akceptací a odstraňování vad



Postup akceptací

- Je-li výsledkem dílčí akceptace „Neakceptováno“ vedoucí projektů jsou povinni zajistit opakování této dílčí akceptace se zahájením v termínu daném schváleným akceptačním protokolem.
- Je-li výsledkem opakované dílčí akceptace „Neakceptováno“ nestanovuje se termín odstranění vad a stav projektu je eskalován na Řídicí výbor, který rozhodne o dalším postupu.
- Je-li výsledkem dílčí akceptace výsledek „Akceptováno s výhradou“ zajistí Hlavní projektový tým realizaci opatření k nápravě nedostatků uvedených v rámci akceptačního vyjádření. Ověření odstranění vad je prováděno v rámci celkové akceptace daného milníku.
- Je-li výsledkem celkové akceptace výsledek „Akceptováno s výhradou“ Vedoucí projektu jsou povinni zajistit opakování akceptace pouze odstraněných vad v termínu daném schváleným akceptačním protokolem.
- Je-li výsledkem celkové akceptace výsledek „Neakceptováno“ Vedoucí projektu jsou povinni zajistit opakování této celkové akceptace se zahájením v termínu daném schváleným akceptačním protokolem. Celková akceptace může být opakována pouze jednou, pokud Řídicí výbor nerozhodne jinak.
- Řídicí výbor rozhodne o dopadech výše uvedených situací postupu akceptací na harmonogram plnění. Řídicí výbor je oprávněn rozhodnout o změně dílčích termínů plnění v rámci kteréhokoliv milníku/etapy, avšak změna termínu ukončení milníku/etap je možná výhradně prostřednictvím dodatku k relevantní smlouvě podepsaného oběma smluvními stranami.

4.7.6. Postup odstraňování vad

Cílem odstranění vad je zajistit předání Díla jak v jednotlivých částech, tak vcelku v podobě a kvalitě, která je plně v souladu s požadavky Specifikace Předmětu plnění a s požadavky a návrhy specifikovanými a odsouhlasenými v průběhu projektu.

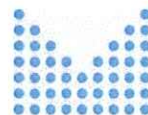
Odstraňování vad musí být plánovanou činností a minimální struktura harmonogramu musí zahrnovat i nezbytné termíny opravných akceptací pro celkovou akceptaci.

Stanovení postupu ověření odstranění vady je v kompetenci Hlavního projektového týmu.

4.8. Issue Management

4.8.1. Issue Log

V rámci Projektu je veden tzv. Issue log, tj. soupis požadavků (předmětu Díla), otevřených problémů, incidentů, změnových požadavků a dalších otevřených situací na Projektu včetně evidence jejich aktuálního stavu zejména s ohledem na stav dodání, akceptace, vad, dodání dokumentace, provedení školení a odkazu na dokumentaci s jejich popisem nebo protokoly identifikovaných a sledovaných projektovým týmem v jeho průběhu, včetně priorit a jejich aktuálního stavu. „Otevřené body“ jsou jednak všechny problémy, incidenty či situace, ke kterým na Projektu dochází a které mají vliv na schválený Plán Projektu a jednak požadavky na změny oproti schválenému rozsahu Projektu.



4.8.2. Řízení požadavků (Issue management)

V průběhu celého Projektu je PM za Dodavatele povinen udržovat aktuální verzi dokumentu Issue log a sledovat stav řešení jednotlivých položek. Jednotlivé položky, navržený způsob a termíny jejich řešení jsou probírány a odsouhlasovány na pravidelných schůzkách HPT.

Celý proces, za který odpovídá PM za stranu Dodavatele, zahrnuje následující aktivity:

- Průběžné sledování stavu dodání a implementace požadavků (předmětu Díla) a evidence stavu v Issue logu.
- Průběžná identifikace nových otevřených problémů, incidentů, změnových požadavků a dalších otevřených situací na Projektu a jejich zaznamenání do Issue logu.
- Rozhodnutí o dopadu, který má každá položka na Dílo (nebo jeho dílčí část).
- Přidělení priority každé nové položce, ev. změna priority stávajících položek.
- Pravidelné sledování stavu řešení jednotlivých položek.
- Zajištění práce na rychlém a kvalitním řešení jednotlivých položek jednotlivými členy projektového týmu.
- Pravidelný reporting o stavu Issue logu směrem k HPT a ŘV v rámci Zprávy o stavu projektu.

4.8.3. Změnové řízení

Pro jednoznačnost obě Smluvní strany potvrzují, že Smlouvou stanovená cena za předmět Smlouvy je konečná a nepřekročitelná. Obsahuje veškeré náklady Dodavatele nutné k řádnému dodání Díla, resp. k realizaci úplného předmětu Smlouvy.

Všechny požadavky na změny schváleného rozsahu Projektu procházejí procesem standardního změnového řízení, které zahrnuje následující aktivity:

- Vypracování návrhu požadavku na změnu, obsahující:
 - Specifikaci návrhu změny.
 - Zdůvodnění a posouzení vztahů a souvislostí se stávajícím Projektem.
- Posouzení dopadu do stávajícího Plánu Projektu v oblasti:
 - Harmonogramu.
 - Rozpočtu.
 - Vlivu změn na již realizované části Projektu.
 - Vlivu změn na ještě nerealizované části Projektu.
 - Vlivu na rozhraní s jinými systémy.
- Schválení požadavku ŘV, resp. zástupci Dodavatele v ŘV.
- Vypracování Dodatku k platné Smlouvě o dílo, je-li to relevantní.
- Naplánování prací na změnových požadavcích na straně Dodavatele.

V případě změn detailů technického projektu (dále jen „ZDTP“) se nejedná se o změnové řízení Projektu, ale o drobné odchylky v detailech technického řešení oproti schválenému Technickému

projektu (bez změny ceny Díla). Inicie ZDTP je povoleno pouze ze strany Objednatele. Mechanismus schvalování ZDTP bude následující:

- popis a zdůvodnění změny,
- návrh řešení,
- schválení změny.

Schválení ZDTP proběhne na jednání schvalovací komise, která bude složena ze zástupců obou smluvních stran. Komise na tomto jednání ZDTP:

- schválí,
- zamítne,
- vrátí k dopracování, pokud vzniknou pochybnosti např. o návrhu řešení.

O ZDTP bude sepsán „Protokol o změně“, který podepíší obě Smluvní strany.

4.9. Záruky

Definice pojmů

BD	Business Day – týž pracovní den
BE	Best Effort – jakmile je to možné, vyvinutí maximální snahy (s vynaložením odborné péče a současného stavu techniky) k co nejrychlejšímu vyřešení požadavku, doba není garantována
NBD	Next Business Day – následující pracovní den
Odezva (response time)	Je časová lhůta, ve které je Poskytovatel povinen odpovědět na požadavek předaný prostřednictvím servis desku Objednatele, a to buď odmítnutím, nebo přijetím požadavku.
Obnovení služby (fix time)	Je časová lhůta, ve které je Poskytovatel povinen obnovit parametry služby na sjednanou úroveň nebo dosáhnout nižší priority požadavku s tím, že doba na obnovení parametrů Služby je počítána od vzniku původního požadavku bez ohledu na změnu kvalifikace priority požadavku.
Doba nástupu na opravu	Je časová lhůta, ve které je Poskytovatel započne práce na obnově parametrů služby na sjednanou úroveň. Jedná se zejména dobu započeti opravy fyzické infrastruktury.
Provozní prostředí	Prostředí Dohledového centra MV pro provoz ICT systémů a kybernetickou bezpečnost
Rozsah poskytování služby (kalendář)	Kdy je služba poskytována – od-do, které dny v týdnu (např. 24x7, 8x5, 10x5). 8x5 – pracovní dny od 8:00 do 16:00 hodin 10x5 – pracovní dny od 8:00 do 18:00 hodin 24x7 – nepřetržitě
Systém	Dohledové centrum MV pro provoz ICT systémů a kybernetickou bezpečnost (SOCCR)

**Stanovení priority incidentů, požadavků pro provozní prostředí**

Priorita požadavku	Definice priority požadavku	Parametry řešení požadavku
Priorita požadavku 1 Kritická	Některé nebo všechny části Systému selhaly a poskytovaná služba je zcela nefunkční nebo je jejich funkčnost omezena tak, že je kritickým způsobem ovlivněna činnost Systému.	Odezva: 30 minut Obnovení služby: 4 hodiny Kalendář: 24x7
Priorita požadavku 2 Vysoká	Systém je funkční pouze částečně. Některé části selhaly a jsou zcela nefunkční nebo je jejich funkčnost omezena tak, že je zásadním způsobem ovlivněna činnost Systému. Je omezena redundance a současně jsou služby poskytovány s vyšší než požadovanou odezvou po dobu delší než 1 hodinu.	Odezva: 1 hodina Obnovení služby: 8 hodin Kalendář: 24x7
Priorita požadavku 3 Střední	Systém je funkční pouze částečně. Je omezena redundance, zejména fyzické infrastruktury.	Odezva: 1 hodina Doba nástupu na opravu: následující pracovní den Kalendář: 8x5
Priorita požadavku 4 Ostatní	Požadavkem je žádost o podání informace (dotaz, vysvětlení).	Odezva: BE Obnovení služby: BE Kalendář: 8x5

4.10. Ostatní

Na základě této Metodiky projektového řízení vznikne v rámci Projektu odsouhlasený dokument Plán Projektu, který je součástí projektové dokumentace. Bude stanovovat, jak je Projekt po celou dobu svého trvání prováděn, sledován a kontrolován.

5. Obsazení projektu na straně Dodavatele

Dodavatel na vyžádání předloží CV jednotlivých členů týmu, aby prokázal jejich kvalifikaci.

6. Etapy plnění a Akceptační kritéria

Tato sekce obsahuje definici jednotlivých součástí předmětu dodávky (v souladu s platnou Smlouvou), které podléhají samostatnému převzetí Objednatele, a tvoří součást Akceptace Díla (viz. Sekce 8 tohoto dokumentu).



6.1. Etapy plnění

Č.	Etapa plnění	Zahájení	Dokončení
Etapy plnění v rámci milníku pro fakturaci č. 1			
1.	Technický projekt – zpracování detailního návrhu Dohledového centra MV pro provoz ICT systémů a kybernetickou bezpečnost. Akceptace Technického projektu (závazná Specifikace Předmětu plnění).	1. 1. 2015	31. 3. 2015
Etapy plnění v rámci milníku pro fakturaci č. 2			
1.	Realizace výběrových řízení – bude upřesněno na základě akceptovaného Technického projektu.	1. 4. 2015	30. 6. 2015
2.	Nákup HW a SW a jeho instalace – bude upřesněno na základě akceptovaného Technického projektu.	1. 4. 2015	30. 6. 2015
3.	Zpracování dokumentace – bude upřesněno na základě akceptovaného Technického projektu.	1. 4. 2015	30. 6. 2015
Etapy plnění v rámci milníku pro fakturaci č. 3			
1.	Implementace technologií a navržených procesů – bude upřesněno na základě akceptovaného Technického projektu.	1. 7. 2015	30. 11. 2015
2.	Akceptační testování navržené infrastruktury – bude upřesněno na základě akceptovaného Technického projektu.	1. 10. 2015	31. 10. 2015
3.	Pilotní provoz a přechod na rutinní provoz – bude upřesněno na základě akceptovaného Technického projektu.	1. 11. 2015	30. 11. 2015

Jednotlivé součásti musí mít přímou vazbu na dokumenty Projektu, kterými probíhá formální převzetí, a na podpisová práva.

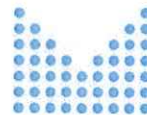
6.2. Akceptační kritéria

6.2.1. Část plnění 1

Technický projekt

Akceptačním kritériem bude odevzdaný Technický projekt Dohledové centrum MV pro provoz ICT systémů a kybernetickou bezpečnost (SOCCR) – Specifikace předmětu plnění, detailní návrh harmonogramu dodávky a návrh všech nezbytných podkladů pro zajištění vypsání Prováděcího projektu VZ vyplývající z potřeb projektu. Prováděcí projekt bude po svém vytvoření ke smlouvě doplněn formou dodatku, který bude podepsán oběma stranami.

Výsledkem Akceptace části plnění 1 bude podepsaný Akceptační protokol č. 1 (viz. vzor v kapitole 6.3).



6.2.2. Část plnění 2

Realizace výběrových řízení

Akceptační kritérium bude úspěšné dokončení všech výběrových řízení potřebných pro dokončení projektu a implementaci celého řešení.

Nákup HW a SW a jeho instalace

Akceptační kritérium bude převzetí HW a SW platformy pro potřeby aplikačního vybavení Dohledové centrum MV pro provoz ICT systémů a kybernetickou bezpečnost (SOCCR) a ověření funkčnosti Objednatelem a podepsání předávacího protokolu.

Zpracování dokumentace

Akceptačním kritériem bude akceptace všech dokumentů potřebných pro úspěšné provozování navrženého řešení (výstupu projektu) a podepsání akceptačního protokolu Objednatelem.

6.2.3. Část plnění 3

Implementace technologií a navržených procesů

Akceptační kritérium bude převzetí naimplementovaných technologií po ověření funkčnosti objednatel (dle prováděcího projektu) a podepsání akceptačního protokolu

Akceptační testování navržené infrastruktury

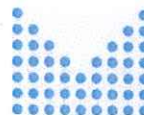
Akceptační kritérium bude dokončení testů (dle prováděcího projektu) a podpis akceptačního protokolu.

Pilotní provoz a přechod na rutinní provoz

Akceptačním kritériem bude dokončení ověřovacího (pilotního provozu) a přechod do rutinního provozování na základě podepsaného závěrečného akceptačního protokolu.

6.3. Vzor akceptačního protokolu

Níže je uvedena ukázka akceptačního protokolu.



AKCEPTAČNÍ PROTOKOL Č.x

Zhotovitel	Česká pošta, s.p., Odštěpný závod ICT služby
Objednatel	Česká republika – Ministerstvo vnitra
Smlouva	
Název Projektu	Zajištění infrastruktury pro operační střediska základních složek IZS
Číslo Projektu	CZ.1.06/1.1.00/07.06414
Datum předání díla	
Předávací protokol č.	

PŘEDMĚT AKCEPTACE

Číslo	Popis	Stav akceptace (Akceptováno; Akceptováno s výhradou; Neakceptováno)
01		
02		
03		

Zhotovitel Česká pošta, s.p., Odštěpný závod ICT služby a Objednatel Česká republika – Ministerstvo vnitra svým podpisem stvrzují Akceptaci předmětu plnění a předání díla, dle Smlouvy o dílo.

Dílo bylo akceptováno na základě Předávacího protokolu č. x ze dne xxxxxx.

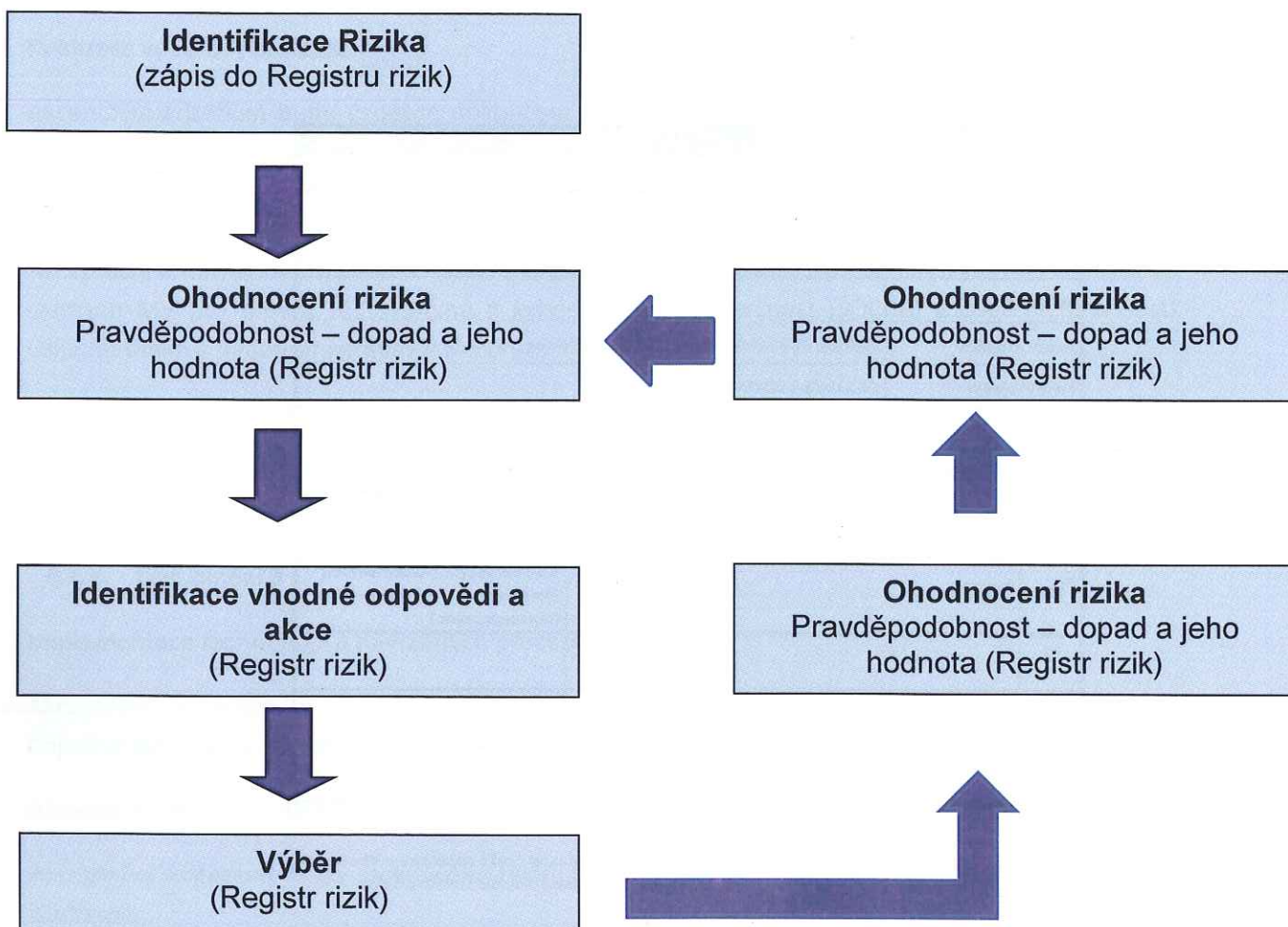
Společnost	Jméno	Podpis
Předal za Českou poštu, s.p., Odštěpný závod ICT služby		
Akceptoval za Českou republika – Ministerstvo vnitra		

Obě strany se dohodly, že toto konstatování formálně nahrazuje Předávací protokol.

7. Řízení rizik

7.1. Řízení rizik

Riziko lze definovat jako nejistotou událost nebo soubor událostí, které pokud nastanou, budou mít dopad na dosažené cíle Projektu. Riziko je měřeno kombinací pravděpodobnosti uvědomění si hrozby nebo příležitosti a závažnosti jeho dopadu na cíle. Řízení rizik pak je procedura, v jejímž průběhu jsou kontinuálně identifikována, vyhodnocována a následně řízena rizika související s projektem. Za řízení rizik je odpovědný Vedoucí projektu Dodavatele, na identifikaci nových rizik se podílí všichni členové projektových týmů.



7.2. Reportování a monitorování rizik

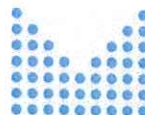
7.2.1. Registr rizik

Pro účely reportingu a monitoringu rizik jsou využívány nástroje v podobě Registru rizik_interní_externí. Registr rizik je soubor formátu xlsx, za jehož vedení je zodpovědný Vedoucí projektu Dodavatele. Za vlastní provedení zaznamenání všech parametrů rizik definovaných v souboru zodpovídá Vedoucí projektu Dodavatele, který je zodpovědný za příjem podnětů, jejich vyhodnocení a rozhodnutí o dalších krocích viz Eskalační procedura rizika.

7.2.2. Eskalace rizik

Tato kapitola obsahuje eskalační procedury v oblasti řízení rizik.

Eskalační procedura	
Interval Významnosti rizika	Proces eskalace (všechny nově identifikovaná rizika (či změna/ vývoj u stávajících) jsou hlášena Vedoucímu projektu Dodavatele.



Eskalační procedura	
	Vedoucí projektu Dodavatele reaguje následovně: • Přijme informaci o novém riziku (popř. eskalaci stávajícího) • Vyhodnotí riziko z hlediska pravděpodobnosti, dopadu a dalších parametrů dle Registru rizik (společně s autorem rizika popř. dalšími relevantními osobami) • Zapiše informace do Registru rizik • Provede vhodnou akci – řešení rizika popř. eskaluje do řídicích struktur projektu
Nově identifikované riziko – úroveň dopadu:	Kterýkoli člen některého z projektových týmů může eskalovat identifikované riziko. O riziku informuje Vedoucího projektu Dodavatele.
1	Riziko nebude eskalováno. Bude postoupeno k vyřešení na úrovni stanoveného projektového týmu.
2	Riziko bude projednáno na standardním jednání Hlavního projektového týmu. Riziko bude postoupeno k vyřešení na úrovni stanoveného projektového týmu.
3	Riziko bude projednáno na mimořádném jednání Hlavního projektového týmu. Riziko bude eskalováno na mimořádném jednání Řídícího výboru projektu. Riziko bude postoupeno k vyřešení na úrovni Hlavního projektového týmu. Pro riziko bude zpracován plán eliminace rizika, který bude předložen Hlavnímu projektovému týmu ke schválení.

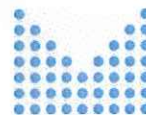
7.2.3. Kategorizace rizik

- Pro vyhodnocení parametrů rizika jsou definovány následující parametry
- Pro účel hodnocení byly definovány následující úrovně dopadu
- Dopad – míra škod způsobených při uskutečnění rizikové události

Významnost	Úroveň dopadu	Úroveň pravděpodobnosti
1	Malá	Téměř nemožné (1% - 20%)
2	Střední	Pravděpodobné (20% - 50%)
3	Zásadní	Velmi pravděpodobné (50% - 90%)

- Pro stanovení rezervy v projektu byl zvolen tento způsob výpočtu:

Rezerva v projektu = pravděpodobnost výskytu X dopad na náklady



- V závislosti na úrovni dopadu rizika bude riziko eskalováno (viz Eskalační procedura) a řízeno. Taktéž na základě úrovně dopadu bude Hlavní projektový tým u mimořádně významných rizik rozhodovat o vypracování detailních postupů eliminace rizika (opatření) popř. havarijních či bezpečnostních plánů
- V parametrech rizika je také sledován dopad na plán při řešení rizika, respektive jeho finanční hodnota

7.3. Návrh registru rizik

Registr rizik bude upřesněn do 10 pracovních dnů po podpisu Smlouvy na základě jednání zástupců Dodavatele a Objednatele.

Struktura Registru rizik bude minimálně následující:

- Název rizika
- Popis rizika
- Plán eliminace
- Plán řešení
- Datum vzniku
- Status rizika
- Dopad na projekt
- Datum uzavření

Registr rizik bude pravidelně aktualizován na jednání HPT.



Vzor rozklad dodávky na položky

Rozklad dodávky na položky:

Číslo	Název	Typ	Výrobní číslo	Množství	Cena za jednotku bez DPH	Cena za jednotku s DPH	Cena celkem bez DPH	Cena celkem s DPH
-------	-------	-----	---------------	----------	--------------------------	------------------------	---------------------	-------------------

HW do 40 000 Kč / jednotku

Celkem

HW nad 40 000 Kč / jednotku

Celkem

SW do 60 000 Kč / jednotku

Celkem

SW nad 60 000 Kč / jednotku

Celkem

Cena celkem za předmět plnění

--	--



Dodaný HW:

PC:

Název	Typ / Popis
Procesor	
Základní deska	
Operační paměť	
Disk pevný	
Mechanika	
Karta grafická	
Karta zvuková	
Karta síťová	
Zdroj	
Multimédia	
Příslušenství	
OS	
SW	
Displej	
Vlastnosti obrazovky	
Rozhraní	



Notebook:

Název	Typ / Popis
Procesor	
Základní deska	
Operační paměť	
Disk pevný	
Grafická karta	
Displej	
Optická mechanika	
Hmotnost	
Zvuková karta	
Multimédia	
Komunikace (WiFi, Ethernet,..)	
Rozhraní	
Příslušenství	
OS	
SW	



Server:

Název	Typ / Popis
Značka	
Typ	
Provedení	
Procesory	
Operační paměť	
Pevné disky	
Rozhraní	
Sloty	
Optická mechanika	
Podpora RAID	
Síť	
Zdroj	
OS	
Záruka	