

SMLOUVA O DÍLO

Článek I. Smluvní strany

objednatel: Česká republika - Ministerstvo vnitra
se sídlem: Praha 7, Nad Štolou 936/3, PSČ 170 34
IČO: 00007064
DIČ: CZ00007064
zastoupen: Mgr. Jaromírem Bischofem, ředitelem Správy logistického zabezpečení Policejního prezidia České republiky
adresa pro doručování: Správa logistického zabezpečení Policejního prezidia ČR, Praha 5, Nádražní 16, PSČ: 150 05, P. O. BOX 6
bankovní spojení: Česká národní banka, pobočka Praha
číslo účtu: 5504881/0710
kontaktní osoba: Ing. Blanka Pospíšilová
telefonní číslo: +420 974 835 447
e-mail: blanka.pospisilova2@pcr.cz

(dále jen „objednatel“)

a

zhotovitel: VISITECH a.s.
se sídlem: Košínova 655/59, Brno-Královo pole, PSČ 612 00
zastoupen: Pavlem Kocourem, předsedou představenstva
IČO: 25543415
DIČ: CZ25543415
číslo účtu: 1017756001/5500
kontaktní osoba: dr. Vašíček Ivo
telefonní číslo: +420 608 240 742
e-mail: ivo.vasicek@visitech.cz

zapsaný v obchodním rejstříku vedeném u Krajského soudu v Brně, oddíl B, vložka 6323

(dále jen „zhotovitel“)

uzavírají podle ust. § 2586 a násl. zákona č. 89/2012Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“) tuto smlouvu o dílo (dále jen „smlouva“).

Článek II. Předmět smlouvy

(1) Předmětem této smlouvy je závazek zhotovitele zhotovit a předat řádně, včas a ve sjednané kvalitě dílo specifikované v odst. 2 a 3 tohoto článku (dále jen „dílo“). Předmětem smlouvy je rovněž závazek objednatele zaplatit zhotoviteli za řádně a včas zhotovené a předané dílo sjednanou cenu.

(2) Specifikace díla: Zpracování aktualizace současné Bezpečnostní politiky odboru informatiky a provozu informačních technologií Policejního prezidia České republiky (dále jen „OIPIT“), která musí navazovat na rezortní bezpečnostní politiku a současně rozvíjet ty oblasti, které jsou specifické pro informační systémy Policie ČR, dále zpracování obecné bezpečnostní dokumentace, pokrývající zejména informační systémy, které jsou zařazeny do kritické informační infrastruktury podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), zejména bude vyhotovena:

- a) aktualizovaná Bezpečnostní politika OIPIT, včetně posouzení kontextu organizace v souladu s normou ISO 31000 a posouzení rizik podle normy ISO 27005
- b) prováděcí bezpečnostní směrnice rozvíjející Bezpečnostní politiku OIPIT do konkrétních procesů naplňujících požadavky Bezpečnostní politiky OIPIT
- c) strategie řízení kontinuity činností Databázového centra Policie ČR
- d) typová bezpečnostní dokumentace informačního systému
- e) směrnice pro provádění interních auditů bezpečnosti informací
- f) směrnice pro testování bezpečnosti
- g) směrnice pro správu a zvládání bezpečnostních incidentů
- h) směrnice pro zálohování, obnovu a testování obnovy.

(3) Dokumentace bude vypracována tak, aby splňovala požadavky na bezpečnostní dokumentaci stanovenou v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve vyhlášce č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti), a v normách řady ISO 27000. Dokumentace musí splňovat požadavek na přizpůsobení organizaci tak, aby popisované procesy a role byly přizpůsobeny organizačnímu členění až na jednotlivé tabulkové pozice. V případě, že realizace požadavku výše uvedené bezpečnostní dokumentace je upravena dalšími interními akty řízení, bude v dokumentaci na tyto dokumenty odkaz, včetně kapitoly, která problematiku řeší. Výstupem rovněž bude doporučení ohledně případného dopracování a sjednocení další bezpečnostní dokumentace OIPIT, bude-li to účelné.

(4) Přesná specifikace prováděných prací je rozepsána v nabídce zhotovitele ze dne 14. června 2016 a v zadávací dokumentaci ze dne 3. června 2016 včetně příloh.

Článek III.

Způsob zhotovení a předání díla

(1) Zhotovitel je při zhotovení díla povinen postupovat s odbornou péčí, podle svých nejlepších znalostí a schopností, přičemž je při své činnosti povinen chránit zájmy a dobré jméno objednatele a postupovat v souladu s jeho pokyny. V případě nevhodných pokynů objednatele je zhotovitel povinen na nevhodnost těchto pokynů objednatele písemně upozornit, v opačném případě nese zhotovitel zejména odpovědnost za vady a za škodu, které v důsledku nevhodných pokynů objednatele objednateli a/nebo zhotoviteli a/nebo třetím osobám vznikly.

- (2) Výsledek činnosti, jenž je předmětem díla nebo jeho části podle této smlouvy, není zhotovitel oprávněn poskytnout třetím osobám ve smyslu ust. § 2633 občanského zákoníku.
- (3) Zhotovitel zpracuje a předá dílo nejpozději do 4 měsíců od podpisu smlouvy.
- (4) Dílo bude provedeno v českém jazyce.
- (5) Místem předání díla je Bubenečská 20, Praha 6. Vlastní výkon prací na díle může probíhat po předchozí vzájemné dohodě i v prostorách objednatele, v pracovních dnech od 8.00 do 14.00 hod. Vlastnické a užívací právo ke zhotovovanému dílu přechází na objednatele okamžikem předání díla objednateli.
- (6) Dílo bude odevzdáno objednateli v počtu tří (3) kompletních sad v listinné podobě a dvakrát (2) v digitální podobě na hmotném nosiči informace (např. nepřepisovatelné CD, DVD apod.), každý s kompletní sadou vyhotovené dokumentace v editovatelném formátu (MS Office).
- (7) Objednatel je oprávněn odmítnout převzetí díla, pokud dílo nebude zhotoveno řádně v souladu s touto smlouvou a ve sjednané kvalitě, přičemž v takovém případě objednatel důvody odmítnutí převzetí díla písemně zhotoviteli sdělí, a to nejpozději do pěti (5) pracovních dnů od termínu předání díla.
- (8) Dodavatel ručí za soulad dokumentace s právní úpravou, vnitřními předpisy a požadovanými normami platnými ke dni předání. Pokud dodavatel bude v době zpracování dokumentace až do jejího předání disponovat informací, že se připravuje změna právní úpravy, norem apod., musí na tuto skutečnost objednatele neprodleně upozornit.
- (9) O předání a převzetí díla zhotovitel vyhotoví protokol ve dvou (2) vyhotoveních, který bude podepsán pověřenými zástupci smluvních stran. Každá ze smluvních stran obdrží po jednom vyhotovení protokolu.

Článek IV. Práva duševního vlastnictví

- (1) Zhotovitel se zavazuje, že při vypracování díla neporuší práva třetích osob, která těmto osobám mohou plynout z práv duševního vlastnictví, zejména z autorských práv a práv průmyslového vlastnictví. Zhotovitel se zavazuje, že objednateli uhradí veškeré výdaje, škody a majetkovou i nemajetkovou újmu, které objednateli vzniknou v důsledku uplatnění práv třetích osob vůči objednateli v souvislosti s porušením povinností zhotovitele dle předchozí věty.
- (2) Zhotovitel prohlašuje, že je oprávněn poskytnout objednateli veškerá práva spojená s realizací této smlouvy a s aplikací díla chráněného podle autorského zákona (dále jen „dílo“). Zhotovitel je povinen zajistit, aby objednatel nabyl příslušná oprávnění z práv duševního vlastnictví, která se týkají díla a která jsou bez dalších podmínek nezbytná pro jeho oprávnění k výkonu práva neomezeného užívání díla.
- (3) Dnem předání a převzetí jakékoliv části plnění, která naplňuje znaky díla, nabývá objednatel na neomezenou dobu výhradní licenci ke všem nezbytným způsobům řádného užití díla a k účelům vyplývajícím z této smlouvy po celou dobu trvání autorských práv k dílu. V rámci poskytnutého užívacího práva zhotovitel uděluje objednateli neodvolatelnou, neomezenou a postupitelnou licenci k veškerým způsobům užití díla. Objednatel je zároveň oprávněn upravit či jinak měnit dílo, jeho název nebo spojit dílo s jiným dílem a zařadit dílo do díla souborného. Objednatel není povinen licenci využít.
- (4) Odměna za poskytnutou licenci je zahrnuta v ceně díla.

Článek V. Cena díla

- (1) Smluvní strany se dohodly, že za dílo řádně zhotovené, předané a převzaté podle této smlouvy objednatel zaplatí zhotoviteli **cenu díla ve výši 518 000,- Kč bez DPH, tj. 626 780,- Kč včetně DPH**, při sazbě DPH ve výši 21%, přičemž sazba DPH bude v případě její změny stanovena v souladu s platnými právními předpisy.
- (2) Tato sjednaná cena díla zahrnuje veškeré výdaje vzniklé zhotoviteli v souvislosti se zhotovením a předáním díla.
- (3) Cena díla bude zaplacená na základě faktury vystavené zhotovitelem po řádném zhotovení a předání díla a jeho převzetí objednatelem. Faktura musí obsahovat náležitosti podle ust. § 29 zákona č. 235/2004 Sb., zákona o dani z přidané hodnoty, ve znění pozdějších předpisů a náležitosti podle ust. § 435 občanského zákoníku. Dále musí faktura obsahovat označení zhotovitele, objednatele a příjemce faktury (Policejní prezidium ČR, poštovní schránka 62/ŘPVS, 170 89 Praha 7). Přílohou faktury bude kopie protokolu o předání a převzetí díla.
- (4) Smluvní strany se dohodly na lhůtě splatnosti faktury v délce třicet (30) kalendářních dnů ode dne prokazatelného doručení faktury příjemci faktury, a to bezhotovostním převodem na bankovní účet zhotovitele uvedený ve smlouvě. Cena díla se považuje za uhrazenou okamžikem odepsání fakturované ceny díla z bankovního účtu objednatele. Pokud objednatel uplatní nárok na odstranění vady díla ve lhůtě splatnosti faktury, není objednatel povinen až do odstranění vady díla uhradit cenu díla. Okamžikem odstranění vady díla začne běžet nová lhůta splatnosti faktury v původní délce.
- (5) Objednatel je oprávněn vrátit bez zaplacení fakturu, která neobsahuje náležitosti stanovené touto smlouvou nebo budou-li tyto údaje uvedeny chybně; faktura se považuje za vrácenou ve lhůtě splatnosti, je-li v této lhůtě odeslána, není nutné, aby byla v téže lhůtě doručena zhotoviteli, který ji vystavil. Zhotovitel je povinen podle povahy nesprávnosti fakturu opravit nebo nově vyhotovit. V takovém případě není objednatel v prodlení se zaplacením ceny díla. Okamžikem doručení náležitě doplněné či opravené faktury začne běžet nová lhůta splatnosti faktury v délce třicet (30) kalendářních dnů.
- (6) Objednatel nebude poskytovat zhotoviteli jakékoliv zálohy na úhradu ceny díla nebo její části.

Článek VI. Kontrola provádění díla

- (1) Zhotovitel je povinen zapracovat do díla připomínky uplatněné objednatelem v průběhu zhotovení díla bez jakéhokoli nároku na zvýšení ceny díla. Zapracování těchto připomínek do díla nesmí vést ke zhoršení kvality zhotovovaného díla.
- (2) Zhotovitel se zavazuje předkládat objednateli na jeho žádost písemné informace o průběhu a obsahu prací v rámci zhotovovaného díla.

Článek VII.

Záruka

- (1) Zhotovitel poskytuje za jakost díla záruku ve smyslu ust. § 2619 občanského zákoníku. Záruční doba je stanovena na jeden (1) rok a začíná plynout ode dne převzetí díla objednatelem.
- (2) Objednatel je oprávněn oznámit vady díla (závady/nesoulad/nedostatky v dokumentaci) a uplatnit nároky z odpovědnosti za vady díla neprodleně po jejich zjištění. Reklamace vad musí být provedena písemně. Pokud objednatel uplatní nárok na odstranění vady díla, zavazuje se zhotovitel tuto vadu bezplatně odstranit nejpozději do deseti (10) pracovních dnů ode dne oznámení vady, nebo ve lhůtě určené objednatelem, pokud by výše uvedená lhůta nebyla přiměřená. O dobu odstraňování vady se prodlužuje záruční doba.
- (3) Odstavec 2 tohoto článku se neuplatní v případech, kdy k nesouladu dokumentace s právními normami došlo změnou právní úpravy nebo normy, o které zhotovitel v době předání díla při vynaložení veškeré péče nemohl vědět.

Článek VIII.

Povinnost mlčenlivosti

- (1) Zhotovitel se zavazuje zachovávat ve vztahu ke třetím osobám mlčenlivost o informacích, které při plnění této smlouvy získá od objednatele nebo o objednateli či jeho zaměstnancích a spolupracovnících a nesmí je zpřístupnit bez písemného souhlasu objednatele žádné třetí osobě ani je použít v rozporu s účelem této smlouvy, ledaže se jedná:
 - a) informace, které jsou veřejně přístupné, nebo
 - b) případ, kdy je zpřístupnění informace vyžadováno zákonem nebo závazným rozhodnutím oprávněného orgánu.
- (2) Zhotovitel je povinen zavázat povinností mlčenlivosti podle odst. 1 tohoto článku všechny osoby, které se budou podílet na zpracování díla.
- (3) Za porušení povinnosti mlčenlivosti osobami, které se budou podílet na zpracování díla, odpovídá zhotovitel, jako by povinnost porušil sám.
- (4) Povinnost mlčenlivosti trvá i po skončení účinnosti této smlouvy.

Článek IX.

Sankční ustanovení a odstoupení od smlouvy

- (1) Za prodlení s termínem předání díla se sjednává jednorázová pokuta ve výši 10 % z ceny díla včetně DPH a dále smluvní pokuta ve výši 0,5 % z ceny díla včetně DPH za každý započatý den prodlení.
- (2) Za prodlení s termínem s odstraněním reklamované vady v záruční lhůtě dle článku VI. smlouvy se sjednává smluvní pokuta ve výši 0,5 % z ceny díla včetně DPH za každý započatý den prodlení s odstraněním vady.
- (3) Za prodlení s úhradou platby faktur bude objednateli účtován zákonný úrok z prodlení z dlužné částky včetně DPH za každý započatý den prodlení.
- (4) Úrok z prodlení a smluvní pokuta jsou splatné do třiceti (30) dnů od data, kdy byla povinné straně doručena písemná výzva k jejich zaplacení stranou oprávněnou, a to na účet oprávněné strany uvedený v písemné výzvě.

- (5) Ustanoveními o smluvní pokutě není dotčeno případné právo objednatele na náhradu škody.
- (6) Objednatel je oprávněn odstoupit od smlouvy zejména v případě, že:
- a) zhotovitel neodevzdá dílo ani v náhradním termínu, který bude objednatelem v rozumné míře nově zhotoviteli stanoven v písemné formě
 - b) zhotovitel neodstraní reklamované vady díla ve stanovené lhůtě nebo v případě, že vady díla nelze odstranit
 - c) proti zhotoviteli bude zahájeno insolvenčního řízení, či zhotovitele vstoupí do likvidace.
- (7) Účinky odstoupení od smlouvy nastávají okamžikem doručení písemného projevu vůle odstoupit od této smlouvy druhé smluvní straně. Odstoupení od smlouvy se nedotýká zejména nároku na náhradu škody a smluvní pokuty.
- (8) Objednatel je oprávněn tuto smlouvu vypovědět i bez uvedení důvodu s patnáctidenní (15) výpovědní lhůtou, která počíná běžet prvního dne po doručení písemné výpovědi zhotoviteli. V takovém případě je zhotovitel povinen učinit již jen takové úkony, bez nichž by mohly být zájmy objednatele vážně ohroženy.

Článek X. Závěrečná ustanovení

- (1) Zhotovitel prohlašuje, že je právnickou osobou zapsanou v obchodním rejstříku; fyzickou osobou podnikající na základě živnostenského oprávnění a splňuje veškeré podmínky a požadavky stanovené právním řádem České republiky a touto smlouvou k plnění předmětu smlouvy. Dále zhotovitel prohlašuje, že disponuje veškerými odbornými, materiálními a technickými předpoklady potřebnými pro splnění smlouvy. Zhotovitel prohlašuje, že ke dni podpisu této smlouvy není v úpadku nebo ve stavu hrozícího úpadku ve smyslu zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů.
- (2) Smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.
- (3) Tato smlouva může být měněna se souhlasem obou smluvních stran pouze písemnou formou označenou jako číslované dodatky.
- (4) Smluvní strany jsou povinny bez zbytečného odkladu oznámit druhé smluvní straně změnu údajů v záhlaví smlouvy.
- (5) Zhotovitel prohlašuje, že dílo nemá právní vady ve smyslu ust. § 1920 a § 2616 občanského zákoníku
- (6) Zhotovitel není oprávněn postoupit smlouvu ani práva a povinnosti ze smlouvy na třetí osobu bez předchozího písemného souhlasu objednatele.
- (7) Zhotovitel bez jakýchkoli výhrad souhlasí se zveřejněním své identifikace a dalších údajů uvedených ve smlouvě včetně ceny díla.
- (8) Ustanovení neupravená touto smlouvou se řídí obecně platnými právními předpisy České republiky, zejména občanským zákoníkem.
- (9) Tato smlouva je vyhotovena ve třech stejnopisech. Jeden obdrží zhotovitel, dva stejnopisy obdrží objednatel.

(10) Smluvní strany prohlašují, že tuto smlouvu uzavírají svobodně a vážně, že si obsah smlouvy přečetly a považují jej za určitý a srozumitelný a že jim jsou známy veškeré skutečnosti, jež jsou pro uzavření této smlouvy rozhodující, na důkaz čehož připojují své vlastnoruční podpisy.

Přílohy této smlouvy:

Příloha č. 1 - Cenová nabídka

V Praze dne14.07.2016

za objednatele:



Mgr. Jaromír Bischof
ředitel SLZ PP ČR
MINISTERSTVO VNITRA ČR
Policejní prezidium ČR
Správa logistického zabezpečení

V Brně dne11.7.2016

za zhotovitele:



Pavel Kocour
předseda představenstva

VISITECH a.s. ①
šínova 59, 612 00 Brno
DIČ: CZ25543415

Příloha č. 1 – cenová nabídka

CENOVÁ NABÍDKA

1. Cenová nabídka

Cenová nabídka za realizaci veřejné zakázky malého rozsahu „Zpracování bezpečnostní politiky systémů“:

Cena díla bez DPH	DPH ve výši 21 %	Cena díla včetně DPH
518 000 Kč	108 780 Kč	626 780 Kč

Nabídková cena je uvedena jako absolutní a nepřekročitelná částka za provedení celkové zakázky a obsahuje veškeré náklady se zakázkou spojené.

2. Specifikace prováděných prací

I ÚVOD

Přístup k realizaci projektu chápeme tak, že zpracované dokumenty musí vyhovovat požadavkům stanoveným v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve vyhlášce č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti), a v normách řady ISO 27000.

Výsledná dokumentace bude přizpůsobena organizaci tak, aby popisované procesy a role odpovídaly organizačnímu členění až na jednotlivé tabulkové pozice. V dokumentaci budou uvedeny odkazy na související akty řízení.

Součástí výstupu bude také doporučení na případné dopracování a sjednocení další bezpečnostní dokumentace OIPIT.

Při akceptaci každé důležité etapy projektu se předpokládá prezentace výstupů a oponentní řízení k předkládaným návrhům výstupů. Vždy bude brán ohled na požadavky zadavatele tak, aby výsledná dokumentace odpovídala jeho podmínkám a požadavkům.

II AKTUALIZACE BEZPEČNOSTNÍ POLITIKY OIPIT

II.1 Vstupní analýza OIPIT

1) Provede se posouzení vnitřního a vnějšího kontextu OIPIT.

- a. Identifikují se požadavky předpisů – zákonných a podzákonných - vždy v platném znění (zákon 273/2008 Sb., zákon 181/2014 Sb., zákon 101/2000 Sb., vyhláška 316/2014 Sb. atd.).

- b. Identifikují se požadavky resortních předpisů (normativních aktů a příkazů Policejního prezidenta a Ministra vnitra ČR a závazné bezpečnostní politiky nadřízených subjektů, které mají vztah k OIPIT).
- c. Identifikují se případné smluvní závazky a další povinnosti, které mohou mít vliv na Bezpečnostní politiku OIPIT.
- d. Identifikují se další závazky (služby), které OIPIT poskytuje, směrem k PČR a případně k MV, nebo které nakupuje od externích dodavatelů.
- e. Proveďte se GAP analýza stávající Bezpečnostní politiky OIPIT, která ukáže, co v BP OIPIT není řešeno a co se musí změnit, nebo doplnit.

Výsledkem činností uvedených v bodech a. až d. bude tabulka požadavků na BP OIPIT.

- 2) Z výše uvedených analýz se provede stanovení kontextu organizace a stanovení rozsahu Bezpečnostní politiky OIPIT a působnosti OIPIT v oblasti řízení bezpečnosti informací.

II.2 Posouzení rizik

Na základě stanoveného rozsahu bezpečnostní politiky OIPIT budou stanovena primární aktiva OIPIT a typová podpůrná aktiva. Posouzení rizik bude provedeno podle metodiky standardu ČSN ISO 27005, kde bude použit přístup k posouzení rizik bezpečnosti informací E. 1 Přehledové posouzení rizik bezpečnosti informací.

Výsledkem posouzení rizik bude stanovení konkrétních parciálních rizik pro jednotlivá aktiva a vybrané hrozby.

Druhým výstupem analýzy rizik bude stanovení účinnosti jednotlivých opatření dle přílohy „A“ standardu ISO 27001. Pro použití v podmínkách zákona o kybernetické bezpečnosti budou jednotlivá opatření standardu ISMS namapována na opatření vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti.

II.3 Presentace výsledků Vstupní analýzy OIPIT

Proběhne presentace výsledků Vstupní analýzy OIPIT, Posouzení rizik, návrhu přístupu k řízení bezpečnosti informací a obsahu Bezpečnostní politiky OIPIT, které budou diskutovány a podle požadavků zadavatele upraveny.

II.4 Aktualizace bezpečnostní politiky OIPIT

Na základě schválených výsledků vstupní analýzy OIPIT proběhne aktualizace dokumentu bezpečnostní politika OIPIT. Dokument se předloží zadavateli k připomínkám a proběhne oponentní řízení, během kterého budou zapracovány požadavky zadavatele. Dokument se zapracovanými připomínkami se předloží vedení zadavatele k akceptaci.

III PROVÁDĚCÍ BEZPEČNOSTNÍ SMĚRNICE

Prováděcí bezpečnostní směrnice bude rozvíjet bezpečnostní politiku OIPIT do konkrétních procesů. Již při tvorbě Bezpečnostní politiky OIPIT budou definovány konkrétní procesy, kterými se politika realizuje. Tyto procesy budou detailně popsány v Prováděcí bezpečnostní směrnici.

Prováděcí bezpečnostní směrnice bude specifikovat jednotlivé procesy, určí jejich vlastníky a odpovědné osoby za jejich realizaci, provozování, kontrolu a měření a vyhodnocování.

IV STRATEGIE ŘÍZENÍ KONTINUITY ČINNOSTI DATABÁZOVÉHO CENTRA POLICIE ČR

Strategie řízení kontinuity činnosti Databázového centra bude založena na provedení analýzy dopadů (BIA, Business Impact Analysis).

V rámci analýzy dopadů budou identifikována aktiva významná pro provoz databázového centra. Tato aktiva budou ohodnocena z hlediska požadavků na dostupnost a maximální tolerovatelné doby výpadku aktiva. Budou identifikovány vzájemné závislosti mezi aktivy a bude vypočítán požadovaný čas obnovy jednotlivých aktiv. Za časů obnovy bude definováno pořadí obnovy jednotlivých aktiv.

Budou rozebrány případy, kdy reálný čas obnovení aktiva bude delší než maximální tolerovatelný čas výpadku aktiva. V těchto případech bude buďto doporučeno technické řešení nápravy, nebo redundance prostředků.

V rámci strategie řízení kontinuity databázového centra budou vybrány nejpravděpodobnější scénáře ohrožení činností centra a tyto scénáře budou vyhodnoceny z hlediska možných dopadů na činnost databázového centra.

Na základě posouzení aktuálního stavu, bude navržena struktura managementu pro řízení kontinuity databázového centra. Budou popsány role a aktivity, které role v rámci řízení kontinuity činnosti budou provádět.

V rámci strategie řízení kontinuity činnosti databázového centra bude také popsána struktura plánů kontinuity.

V TYPOVÁ BEZPEČNOSTNÍ DOKUMENTACE INFORMAČNÍHO SYSTÉMU

Typová bezpečnostní dokumentace systému bude svojí strukturou vycházet z přílohy č. 4 k vyhlášce č. 316/2014 Sb., a z ustanovení bezpečnostní politiky OIPIT.

V.1 Typová bezpečnostní politika systému

Bude zpracována typová bezpečnostní politika systému, která bude obsahovat bezpečnostní politiky z vyhlášky č.316/2014 Sb., které budou uvedeny ve formě jednotlivých kapitol. Typová bezpečnostní politika bude obsahovat následující kapitoly:

- 1) Politika systému řízení bezpečnosti informací,
- 2) Politika organizační bezpečnosti,
- 3) Politika řízení dodavatelů,
- 4) Politika klasifikace aktiv,
- 5) Politika bezpečnosti lidských zdrojů,
- 6) Politika řízení provozu komunikací,
- 7) Politika řízení přístupu,
- 8) Politika bezpečného chování uživatelů,
- 9) Politika zálohování a obnovy,
- 10) Politika bezpečného předávání a výměny informací,
- 11) Politika řízení technických zranitelností,
- 12) Politika bezpečného používání mobilních zařízení,
- 13) Politika poskytování a nabývání licencí programového vybavení a informací,
- 14) Politika ochrany osobních údajů,
- 15) Politika fyzické bezpečnosti,
- 16) Politika bezpečnosti komunikační sítě,
- 17) Politika ochrany před škodlivým kódem,

- 18) Politika nasazení a používání nástroje pro detekci chyb a kybernetických bezpečnostních událostí,
- 19) Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí,
- 20) Politika bezpečného používání kryptografických ochrany.

V rámci této politiky, tam, kde je to použitelné, budou přednostně použity u OIPIT již zavedené procesy a postupy. V případech, kdy postupy zavedené OIPIT budou v rozporu se vyhláškou č. 316/2014 Sb., budou v politice upřednostněny přístupy definované touto vyhláškou.

Obsah jednotlivých politik bude vycházet z vyhlášky o kybernetické bezpečnosti a v rámci detailních postupů budou použity popisy bezpečnostních opatření ze standardu ISO IEC 27002.

V.2 Další dokumentace

Další dokumentace bude, stejně jako bezpečnostní politika, svojí strukturou vycházet z přílohy č. 4 k vyhlášce č. 316/2014 Sb., a z ustanovení bezpečnostní politiky OIPIT.

Bude zpracována následující typová dokumentace:

- 1) Zpráva z auditu kybernetické bezpečnosti (vzor dokumentu),
- 2) Zpráva z přezkoumání systému řízení bezpečnosti informací (vzor dokumentu),
- 3) Metodika pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik (popis metodiky),
- 4) Zpráva ohodnocení aktiv a rizik (vzor dokumentu),
- 5) Prohlášení o aplikovatelnosti (vzor dokumentu),
- 6) Plán zvládání rizik (vzor dokumentu),
- 7) Plán rozvoje bezpečnostního povědomí (vzor dokumentu),
- 8) Zvládání kybernetické bezpečnostních incidentů (typový dokument popisující zásady a procesy, který musí být upřesněn pro konkrétní informační systém),
- 9) Strategie řízení o kontinuity činnosti (typový dokument popisující zásady a procesy, který musí být upřesněn pro konkrétní informační systém),
- 10) Přehled obecně závazných právních předpisů vnitřních předpisů jiných předpisů smluvních závazků (přehled aktuálně platných dokumentů).

I v případě těchto dokumentů budou upřednostňovány již zavedené postupy u OIPIT, pokud nebudou v rozporu s vyhláškou o kybernetické bezpečnosti.

V.3 Schvalování typové bezpečnostní dokumentace informačního systému

Celá sada výše uvedených dokumentů bude podrobena oponentnímu řízení se zadavatelem, v rámci něhož budou projednány všechny připomínky a zapracovány úpravy do dokumentace tak, aby co nejdéle vyhověla požadavkům zadavatele.

VI SMĚRNICE PRO PROVÁDĚNÍ INTERNÍCH AUDITŮ BEZPEČNOSTI INFORMACÍ

Bude zpracována typová směrnice interních auditů bezpečnosti informací, která vychází s požadavků vyhlášky č. 316/2014 Sb., norem ISO 27001 a 19011. V typové směrnici budou stanovena základní pravidla pro provádění činnosti při:

- 1) plánování,
- 2) provádění, a
- 3) vyhodnocování interních auditů bezpečnosti informací.

Budou stanoveny základní odpovědnosti a pravomoci pro jednotlivé role (manažera kybernetické bezpečnosti, vedoucího auditora a auditora) v rámci provádění interních auditů bezpečnosti informací. V dokumentu budou definovány požadavky na:

- 1) výběr,
- 2) kvalifikaci, a
- 3) výcvik auditora kybernetické bezpečnosti.

Součástí dokumentu budou vzory dokumentů zpracovávané při provádění interních auditů. Jedná se o tyto vzory:

- 1) Roční program auditů (vzor dokumentu),
- 2) Plán interního auditu (vzor dokumentu),
- 3) Zpráva z auditu kybernetické bezpečnosti (vzor dokumentu).

I v případě tohoto dokumentu budou upřednostňovány již zavedené postupy u OIPIT, pokud nebudou v rozporu s vyhláškou o kybernetické bezpečnosti.

VII SMĚRNICE PRO TESTOVÁNÍ BEZPEČNOSTI

Bude zpracována typová směrnice pro testování bezpečnosti informačních systémů, která bude stanovovat základní pravidla pro plánování testování bezpečnosti, použití testovacích metod, jejich vyhodnocování a stanovení výstupů vyhodnocení testování bezpečnosti.

Budou stanovena pravidla a odpovědnosti pro přijímání opatření na základě výsledků testování bezpečnosti informačních systémů.

V dokumentu budou dále stanoveny základní odpovědnosti a pravomoci pro jednotlivé role v rámci testování bezpečnosti.

I v případě tohoto dokumentu budou upřednostňovány již zavedené postupy u OIPIT, pokud nebudou v rozporu s vyhláškou o kybernetické bezpečnosti.

VIIISMĚRNICE PRO SPRÁVU A ZVLÁDÁNÍ BEZPEČNOSTNÍCH INCIDENTŮ

Bude zpracována typová směrnice pro správu a zvládání bezpečnostních incidentů, která bude popisovat základní pravidla a odpovědnosti v rámci řízení bezpečnostních událostí a incidentů. Jednotlivá pravidla budou zpracována v souladu s požadavky vyhlášky č. 316/2014 Sb.

V dokumentu budou definovány jednotlivé kroky při zvládání bezpečnostních událostí a incidentů, aktivace týmu pro řešení kybernetických bezpečnostních událostí, dále pravidla pro komunikaci s Národním bezpečnostním úřadem a reakci na opatření vydané tímto NBÚ.

Dokument bude obsahovat stanovení rolí, pravomocí a odpovědností v rámci řešení bezpečnostních událostí a incidentů.

I v případě tohoto dokumentu budou upřednostňovány již zavedené postupy u OIPIT, pokud nebudou v rozporu s vyhláškou o kybernetické bezpečnosti.

IX SMĚRNICE PRO ZÁLOHOVÁNÍ, OBNOVU A TESTOVÁNÍ OBNOVY

Bude zpracována typová směrnice pro zálohování, obnovu a testování obnovy vycházející z politiky kontinuity činností.

Dokument bude stanovovat základní pravidla pro tvorbu:

- 1) plánu zálohování,
- 2) havarijních plánů, a
- 3) plánů obnovy.

V dokumentu budou dále stanoveny odpovědnosti jednotlivých rolí při tvorbě plánů.

Součástí dokumentu budou vzory dokumentů. Jedná se o tyto vzory:

- 1) Plán zálohování (vzor dokumentu),
- 2) Havarijní plán a plán obnovy (vzor dokumentu).

I v případě tohoto dokumentu budou upřednostňovány již zavedené postupy u OIPIT, pokud nebudou v rozporu s vyhláškou o kybernetické bezpečnosti.