MV-146598-24/KAP 2014

MVCRP014Y8ZN

Dodatek č. 3

ke smlouvě o poskytování služeb
č.j. MV-139045-6/KAP-2011 (dále jen Smlouva) uzavřené dne 27. 5. 2013

1. Smluvní strany:

Dodavatel:

NEWPS.CZ s.r.o.

Sídlem: **Přemyslovská 2845/43, Praha 3, PSČ 130 00**

IČO: **25625632**

DIČ: **CZ25625632**

Zapsaný: **u Městského obch. soudu v Praze, oddíl C, vložka číslo 55889**

Zastoupený: **Ing. Martin Řehořek, jednatel společnosti**

Bankovní spojení: **Raiffeisenbank, a.s., Olbrachtova 9/2006, 140 21 Praha 4**

Číslo účtu: **5081103433 / 5500**

a

Odběratel:

Česká republika – Ministerstvo vnitra

Sídlem: **Nad Štolou 936/3, Praha 7, 170 34**

IČO: **00007064**

DIČ: **CZ00007064**

Jejímž jménem jedná: **Ing. Jiří Kolda, ředitel odboru koncepce, architektury a projektů informačních a komunikačních technologií**

Kontaktní adresa: **Nám. Hrdinů 1634/3, 140 21 Praha 4**

Bankovní spojení: **ČNB, pobočka 701**

Číslo účtu: **6015-3605881/0710**

Dále jen „smluvní strany".

Vzhledem k tomu, že

odběratel potřebuje zajistit

- správu, podporu a údržbu centrály Czech POINT i pro funkcionality a komponenty vytvořené po 27. 5. 2013,
- správu změn systému Czech POINT a vytvoření komplexní dokumentace systému,
- rekonstrukci a modernizaci webových stránek systému Czech POINT,

dohodly se smluvní strany na uzavření tohoto Dodatku č. 3.

2. Příloha č. 1 Smlouvy se mění a nově zní takto:

Příloha č. 1 – Seznam funkcionalit a komponent Systému Czech POINT

1. *Aplikace Czech POINT – Dodavatelem je společnost Software602 a.s., Hornokrčská 15, 140 00 Praha 4, IČ 63078236;*
2. *Výpis z Katastru nemovitostí (KN) – Dodavatelem je společnost Software602 a.s., Hornokrčská 15, 140 00 Praha 4, IČ 63078236;*
3. *Výpis z Obchodního rejstříku (OR) – Dodavatelem je společnost Software602 a.s., Hornokrčská 15, 140 00 Praha 4, IČ 63078236;*
4. *Výpis z Živnostenského rejstříku (ŽR) – Dodavatelem je společnost Software602 a.s., Hornokrčská 15, 140 00 Praha 4, IČ 63078236;*
5. *Výpis z Rejstříku trestů (RT) – Dodavatelem je společnost Deltax system a.s., Jankovcova 1569/2c, 170 00 Praha 7, IČ 49241451;*
6. *Přijetí podání podle živnostenského zákona (§72) – Dodavatelem je společnost Deltax system a.s., Jankovcova 1569/2c, 170 00 Praha 7, IČ 49241451;*
7. *Žádost o výpis nebo opis z Rejstříku trestů podle zákona č.124/2008 Sb. (VRT) - Dodavatelem je společnost Deltax system a.s., Jankovcova 1569/2c, 170 00 Praha 7, IČ 49241451;*
8. *Výpis z bodového hodnocení řidiče (BODY) – Dodavatelem je společnost Software602 a.s., Hornokrčská 15, 140 00 Praha 4, IČ 63078236;*
9. *Vydání ověřeného výstupu ze Seznamu kvalifikovaných Dodavatelů (SKD) – Dodavatelem je společnost ASD Software, s.r.o., Žerotínova 2981/55A, 787 01 Šumperk, IČ 623 63 930;*
10. *Podání do registru účastníků provozu modulu autovraků ISOH (ISOH) – Dodavatelem je společnost Deltax system a.s., Jankovcova 1569/2c, 170 00 Praha 7, IČ 49241451;*
11. *Hlášení nesouladu předložených dokladů na kontaktních místech Czech POINT – Dodavatelem je společnost Software602 a.s., Hornokrčská 15, 140 00 Praha 4, IČ 63078236;*
12. *Napojení matričních úřadů na Centrálu Czech POINT – Dodavatelem je společnost KOMIX s.r.o., Radlická 751/113e, 150 00 Praha 5, IČ 47117087;*
13. *Centrální asistent Systému Czech POINT – Dodavatelem je společnost DATRON, a.s., Vachkova 3008, 470 01 Česká Lípa, IČ 43227520;*
14. *Samoobslužné rozhraní pro správu identit uživatelů – Dodavatelem je společnost Novell Professional Services Česká republika, s.r.o., Na Žertvách 29/2247, 180 00 Praha 8, IČ 25625632;*
15. *POWER User Forum Systému Czech POINT – Dodavatelem je společnost Továrna na dokonalé programy, s.r.o., Bohuňova 1366, 140 00 Praha 4, IČ 45272638;*
16. *Kolektor terénních dat prostřednictvím Systému Czech POINT – Dodavatelem je společnost Software602 a.s., Hornokrčská 15, 140 00 Praha 4, IČ 63078236;*
17. *SMS navigace – Dodavatelem je společnost AutoCont CZ a.s., Poděbradská 55/88, 198 00 Praha 9, IČ 476 76 795;*
18. *Auditní software Centrály Czech POINT – Dodavatelem je společnost Novell Professional Services Česká republika, s.r.o., Na Žertvách 29/2247, 180 00 Praha 8, IČ 25625632;*

19. Manuální výpis z rejstříku trestů – Dodavatelem je společnost Deltax system a.s., Jankovcova 1569/2c, 170 00 Praha 7, IČ 49241451;
20. Výpis z Insolvenčního rejstříku (ISIR) – Dodavatelem je společnost CCA Group a.s., Karlovo nám. 17, 120 00 Praha 2, IČ 25695312;
21. Úschovna Centrály Czech POINT – Dodavatelem je společnost DATRON, a.s., Vachkova 3008, 471 01 Česká Lípa, IČ 43227520;
22. Aplikační vrstva pro konverzi dokumentů (AVK) – Dodavatelem je společnost Profinit, s.r.o., Praha 6, Tychonova 2, PSČ 160 00, IČ 25650203;
23. Centrální úložiště ověřovacích doložek Centrály Czech POINT – Dodavatelem je společnost Novell Professional Services Česká republika, s.r.o., Na Žertvách 29/2247, 180 00 Praha 8, IČ 25625632;
24. Agendy související se zajištěním provozu ISDS na kontaktních místech Czech POINT (AgISDS) – Dodavatelem je společnost Software602 a.s., Hornokrčská 15, 140 00 Praha 4, IČ 63078236;
25. Konektor Centrály Systému Czech POINT na spisovou službu MV ČR – Dodavatelem je společnost Software602 a.s., Hornokrčská 15, 140 00 Praha 4, IČ 63078236;
26. Rozhraní Czech POINT@office – Dodavatelem je společnost Novell Professional Services Česká republika, s.r.o., Na Žertvách 29/2247, 180 00 Praha 8, IČ 25625632;
27. Administrativní modul kontaktních míst Czech POINT – Dodavatelem je společnost Software602 a.s., Hornokrčská 15, 140 00 Praha 4, IČ 63078236;
28. Agenda „Dědictví" v Systému Czech POINT (ISND) – Dodavatelem je společnost KOMIX s.r.o., Radlická 751/113e, 150 00 Praha 5, IČ 47117087;
29. Internetové kontaktní místo veřejné správy Czech POINT (IKM) – Dodavatelem je společnost ALWIL Trade, spol. s r.o., Průběžná 2397/76, 100 00 Praha 10, IČ 16188641;
30. Katalog autentizačních a autorizačních služeb Jednotného Identitního Prostoru Czech POINT (JIP) – Dodavatelem je společnost Novell Professional Services Česká republika, s.r.o., Na Žertvách 29/2247, 180 00 Praha 8, IČ 25625632;
31. Systém DONEZ – Dodavatelem je společnost Software602 a.s., Hornokrčská 15, 140 00 Praha 4, IČ 63078236.
32. Úprava funkcionalit Czech POINT - Dodavatelem je společnost NEWPS.CZ s.r.o., Na žertvách 29/2247, 180 00 Praha 8, IČ 25625632;
33. Úprava komunikačního prostředí a formulářů pro matriční události a ISEO - Dodavatelem je společnost KOMIX s.r.o., Radlická 751/113e, 150 00 Praha 5, IČ 47117087
34. Nové funkcionality Czech POINT 2012 - Dodavatelem je společnost NEWPS.CZ s.r.o., Na žertvách 29/2247, 180 00 Praha 8, IČ 25625632;
35. Dodávka a implementace formulářů Czech POINT - Dodavatelem je společnost Software602 a.s., Hornokrčská 15, 140 00 Praha 4, IČ 63078236;
36. SW modul pro ověření certifikátů podpisů - Dodavatelem je společnost NEWPS.CZ s.r.o., Na žertvách 29/2247, 180 00 Praha 8, IČ 25625632;
37. Bezpečnostní úprava JIP - Dodavatelem je společnost NEWPS.CZ s.r.o., Na žertvách 29/2247, 180 00 Praha 8, IČ 25625632;
38. Formulář pro výpis z CRŘ pro držitele datové schránky - Dodavatelem je společnost Software602 a.s., Hornokrčská 15, 140 00 Praha 4, IČ 63078236.

3. Správa změn systému Czech POINT a vytvoření komplexní dokumentace systému, podrobná specifikace je uvedena v příloze č. 1 tohoto dodatku.

4. Rekonstrukce a modernizace webových stránek systému Czech POINT zahrnující jejich úpravu, podrobná specifikace je uvedena v příloze č. 2 tohoto dodatku.

5. Cena

Celková cena za předmět plnění tohoto dodatku je dohodnuta oběma smluvními stranami ve výši

25 460 000 Kč bez DPH

při sazbě 21% činí DPH 5 346 600 Kč

30 806 600 Kč včetně DPH

a) cena za předmět tohoto dodatku podle bodu 2. je stanovena takto:

- aktivační poplatek ve výši 5 280 000 Kč bez DPH, který je splatný ke dni podpisu smlouvy podle platebních podmínek článku 6 Smlouvy,
- navýšení měsíční platby podle článku 5.2 Smlouvy o částku 440.000,- Kč bez DPH po dobu platnosti prvních 24 měsíců tohoto dodatku, počínaje 1. lednem 2016.
- navýšení měsíční platby podle článku 5.2 Smlouvy o částku 255.000,- Kč bez DPH po uplynutí prvních 24 měsíců tohoto dodatku, počínaje 1. lednem 2018.

b) cena za předmět tohoto dodatku podle bodu 3. je stanovena ve výši 3 000 000 Kč bez DPH. Dnem zdanitelného plnění je den předání této části plnění způsobem uvedeným v příloze č. 1 tohoto dodatku a podle platebních podmínek článku 6 Smlouvy.

c) cena za předmět tohoto dodatku podle bodu 4. je stanovena ve výši 500 000 Kč bez DPH. Dnem zdanitelného plnění je den předání této části plnění způsobem uvedeným v příloze č. 2 tohoto dodatku a podle platebních podmínek článku 6 Smlouvy.

6. Místo a doba plnění je uvedena v článku 3 Smlouvy.

7. Požadavek na součinnost ze strany Odběratele se řídí podle článku 4 Smlouvy.

8. Sankční podmínky

a) Sankční podmínky pro předmět tohoto dodatku podle bodu 2. se řídí ustanoveními článku 7 Smlouvy.

b) Sankční podmínky pro předmět tohoto dodatku podle bodu 3.

Odběratel je oprávněn vystavit sankční fakturu Dodavateli v případě nedodržení termínu plnění ve výši 10.000,- Kč za každý, byť započatý, den prodlení;

c) Sankční podmínky pro předmět tohoto dodatku podle bodu 4.

Odběratel je oprávněn vystavit sankční fakturu Dodavateli v případě nedodržení termínu plnění ve výši 3.000,- Kč za každý, byť započatý, den prodlení;

9. Ostatní ustanovení Smlouvy včetně jejích dodatků č. 1 a 2 zůstávají nezměněny.

10. Dodatek se vyhotovuje v 5 stejnopisech, z nichž Odběratel obdrží tři (3) a Dodavatel dva (2).

11. Dodatek nabývá platnosti a účinnosti dnem podpisu poslední ze zúčastněných stran.

12. Přílohy

V následujících přílohách je podrobná specifikace stanovena v zadávací dokumentaci.

Příloha č. 1 – Správa změn systému Czech POINT a vytvoření dokumentace systému
Příloha č. 2 – Rekonstrukce a modernizace webových stránek Czech POINT.

Výše uvedená Příloha č. 1 se stává Přílohou č. 2 Smlouvy a Příloha č. 2 se stává Přílohou č. 3 Smlouvy.

13. Podpisová strana

	Dodavatel	Odběratel
	V Praze	V Praze
Datum	15. 12. 2015	15 -12- 2015
Jméno	Ing. Martin Řehořek	Ing. Jiří Kolda
Podpis		
Funkce	jednatel	ředitel odboru

Správa změn systému Czech POINT a vytvoření dokumentace k systému

Zadavatel žádá o vytvoření dokumentace k systému Czech POINT podle níže uvedeného vzoru struktury dokumentace a provádění její průběžné aktualizace. Pro dokumenty, jejichž vytvoření je v kompetenci Ministerstva vnitra, je požadováno poskytnutí případné součinnosti dodavatele při jejich zpracování a aktualizaci. Dále zadavatel žádá o vytvoření správy změn dokumentace a aplikačního vybavení systému.

Požadavky na dokumentaci vychází zejména z Vyhlášky č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy) a z Vyhlášky 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).

Dokumentace (zejména v části Provozní dokumentace) nemusí nutně mít uvedenou strukturu, ale měla by obsahovat všechny uvedené obsahové celky.

Zadavatel žádá navrhnout a implementovat Proces (politiku) řízení změn (verzování, schvalovací proces) a zajistit pro uvedenou dokumentaci a aplikační vybavení systému bezpečné elektronické úložiště s řízeným přístupem.

Smluvní strany budou povinny poskytnout si navzájem veškerou součinnost, která se v průběhu plnění projeví jako potřebná. Zadavatel požaduje průběžné předávání vytvořených dokumentů a jejich zavádění do správy dokumentů systému Czech POINT. Předání a převzetí jednotlivých dokumentů bude potvrzeno předávacím protokolem podepsaným pověřenými zástupci obou smluvních stran. Vytvoření kompletní dokumentace k systému a zavedení procesu správy změn je požadováno realizovat nejpozději do 30. 6. 2016.

Vzor struktury dokumentace

I. Projektová dokumentace

1. Zápisy z porad
2. Požadavkové listy
3. Akceptační protokoly
4. Ostatní

II. Provozní dokumentace:

A. systémová příručka

1. **popis funkcí, včetně bezpečnostních, které používá správce systému pro provádění určených činností v ISVS, a návod na použití těchto funkcí,**

pozn.: Dokument, který popisuje funkce (služby) systému.

2. **parametry kvality, které vycházejí z požadavků na kvalitu podle § 3 odst. 2,**

pozn.: Definice provozních parametrů systému, nap. výkonnostních (limitních).

3. **podrobný popis ISVS nebo odkaz na dokument, ve kterém je popis uveden a který je správci systému dostupný,**

pozn.: Architektura (design) systému, datový model, popis procesů, co a kam se loguje, popis vnějších rozhraní (jak vlastních, tak napojení na externí), monitorovací nástroje, statistické výstupy. Mj. tedy popis API KzMÚ, WS JIP/KAAS, napojení na spisovou službu, úložiště ověřovacích doložek.

4. **popis jednotlivých činností vykonávaných při správě informačního systému veřejné správy, včetně činností definovaných pro role podle § 12, určení fyzických osob, které tyto činnosti vykonávají, a oprávnění nezbytných pro výkon těchto činností,**

pozn.: „Administrátorská dokumentace", tedy dokument, který popisuje činnosti administrátorů systému (všech jeho částí) a to jak při rutinním provozu, tak i při obnově běhu systému v případě havárie. Např. plán zálohování, havarijní plány, provozní příručka, instalační příručka, mapa infrastruktury.

5. **definování uživatelů nebo skupin uživatelů a jejich oprávnění a povinnosti při využívání informačního systému veřejné správy.**

pozn.: Popis rolí a oprávnění interních i externích uživatelů. OVM definuje pro ISVS vždy alespoň roli a) správce systému, kterým je zaměstnanec nebo jiná fyzická osoba, která zajišťuje řízení provozu ISVS, b) bezpečnostního správce systému, kterým je zaměstnanec nebo jiná fyzická osoba, která zajišťuje kontrolu bezpečnosti ISVS; zároveň definuje pro každou roli souhrn určených činností a potřebných oprávnění pro provádění těchto činností v ISVS.

B. uživatelská příručka

1. **popis funkcí, včetně bezpečnostních, které používá uživatel pro svou činnost v ISVS, a návod na použití těchto funkcí,**

pozn.: Uživatelská dokumentace, např. příručka pro národního administrátora, lokálního administrátora, prohlížeče krizového řízení, administrátora krizového řízení, administrátora zřizované organizace, uživatele, garanta AIS, návody na použití formulářů registraci AIS

2. **b) vymezení oprávnění a povinností uživatelů ve vztahu k ISVS.**

pozn.: např. Provozní řád

III. bezpečnostní dokumentace

Pozn.: Níže je uvedena kompletní struktura bezpečnostní dokumentace, jak bude vyžadována pro součást kritické informační infrastruktury od května 2016. Pro aktuální stav doporučujeme jako mít minimálně Bezpečnostní politiku a bezpečnostní směrnice pro vybrané součásti systému / činnosti (např. zabezpečení uživatelských účtů, řízení přístupu ext. aplikací k webovým službám, řízení vzdáleného přístupu na servery)

A. Bezpečnostní politika

1. Politika systému řízení bezpečnosti informací

[§ 5 odst. 1 písm. a), § 5 odst. 2 písm. a)]

a) Cíle, principy a potřeby řízení bezpečnosti informací.

b) Rozsah a hranice systému řízení bezpečnosti informací.

c) Pravidla a postupy pro řízení dokumentace.

d) Pravidla a postupy pro řízení zdrojů a provozu systému řízení bezpečnosti informací.

e) Pravidla a postupy pro provádění auditů kybernetické bezpečnosti.

f) Pravidla a postupy pro přezkoumání systému řízení bezpečnosti informací.

g) Pravidla a postupy pro nápravná opatření a zlepšování systému řízení bezpečnosti informací.

2. Politika organizační bezpečnosti

[§ 5 odst. 1 písm. b), § 5 odst. 2 písm. b)]

a) Určení bezpečnostních rolí a jejich práv a povinností,

1. práva a povinnosti manažera kybernetické bezpečnosti,
2. práva a povinnosti architekta kybernetické bezpečnosti,
3. práva a povinnosti auditora kybernetické bezpečnosti,
4. práva a povinnosti garanta aktiv,
5. práva a povinnosti výboru pro řízení kybernetické bezpečnosti.

b) Požadavky na oddělení výkonu činností jednotlivých bezpečnostních rolí.

3. Politika řízení dodavatelů

[§ 5 odst. 1 písm. c), § 5 odst. 2 písm. c)]

a) Pravidla a principy pro výběr dodavatelů.

b) Pravidla pro hodnocení rizik dodavatelů.

c) Náležitosti smlouvy o úrovni služeb a způsobů a úrovní realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti.

d) Pravidla pro provádění kontroly zavedení bezpečnostních opatření.

e) Pravidla pro hodnocení dodavatelů.

4. Politika klasifikace aktiv

[§ 5 odst. 1 písm. d), § 5 odst. 2 písm. d)]

a) Identifikace, hodnocení a evidence primárních aktiv

1. určení a evidence jednotlivých primárních aktiv včetně určení jejich garanta,
2. hodnocení důležitosti primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti.

b) Identifikace, hodnocení a evidence podpůrných aktiv

1. určení a evidence jednotlivých podpůrných aktiv včetně určení jejich garanta,
2. určení vazeb mezi primárními a podpůrnými aktivy.

c) Pravidla ochrany jednotlivých úrovní aktiv

1. způsoby rozlišování jednotlivých úrovní aktiv,
2. pravidla pro manipulaci a evidenci aktiv podle úrovní aktiv,
3. přípustné způsoby používání aktiv.

d) Způsoby spolehlivého smazání nebo ničení technických nosičů dat.

5. Politika bezpečnosti lidských zdrojů

[§ 5 odst. 1 písm. e), § 5 odst. 2 písm. e)]

a) Pravidla rozvoje bezpečnostního povědomí a způsoby jeho hodnocení

1. způsoby a formy poučení uživatelů,
2. způsoby a formy poučení garantů aktiv,
3. způsoby a formy poučení administrátorů,
4. způsoby a formy poučení dalších osob zastávajících bezpečnostní role.

b) Bezpečnostní školení nových zaměstnanců.

c) Pravidla pro řešení případů porušení bezpečnostní politiky systému řízení bezpečnosti informací.

d) Pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice.

1. vrácení svěřených aktiv a odebrání práv při ukončení pracovního vztahu,
2. změna přístupových oprávnění při změně pracovní pozice.

6. Politika řízení provozu a komunikací

[§ 5 odst. 1 písm. f), § 5 odst. 2 písm. f)]

a) Pravomoci a odpovědnosti spojené s bezpečným provozem.

b) Postupy bezpečného provozu.

c) Požadavky a standardy bezpečného provozu.

d) Řízení technických zranitelností.

e) Pravidla a omezení pro provádění auditů kybernetické bezpečnosti a bezpečnostních testů.

7. Politika řízení přístupu

[§ 5 odst. 1 písm. g), § 5 odst. 2 písm. g)]

a) Princip minimálních oprávnění/potřeba znát (need to know).

b) Požadavky na řízení přístupu.

c) Životní cyklus řízení přístupu.

d) Řízení privilegovaných oprávnění.

e) Řízení přístupu pro mimořádné situace.

f) Pravidelné přezkoumání přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách.

8. Politika bezpečného chování uživatelů

[§ 5 odst. 1 písm. h), § 5 odst. 2 písm. h)]

a) Pravidla pro bezpečné nakládání s aktivy.

b) Bezpečné použití přístupového hesla.

c) Bezpečné použití elektronické pošty a přístupu na internet.

d) Bezpečný vzdálený přístup.

e) Bezpečné chování na sociálních sítích.

f) Bezpečnost ve vztahu k mobilním zařízením.

9. Politika zálohování a obnovy

[§ 5 odst. 1 písm. i), § 5 odst. 2 písm. i)]

a) Požadavky na zálohování a obnovu.

b) Pravidla a postupy zálohování.

c) Pravidla bezpečného uložení záloh.

d) Pravidla a postupy obnovy.

e) Pravidla a postupy testování zálohování a obnovy.

10. Politika bezpečného předávání a výměny informací

[§ 5 odst. 1 písm. j)]

a) Pravidla a postupy pro ochranu předávaných informací.

b) Způsoby ochrany elektronické výměny informací.

c) Pravidla pro využívání kryptografické ochrany.

11. Politika řízení technických zranitelností
[§ 5 odst. 1 písm. k)]
a) Pravidla pro omezení instalace programového vybavení,
b) Pravidla a postupy vyhledávání opravných programových balíčků,
c) Pravidla a postupy testování oprav programového vybavení,
d) Pravidla a postupy nasazení oprav programového vybavení.

12. Politika bezpečného používání mobilních zařízení
[§ 5 odst. 1 písm. l)]
a) Pravidla a postupy pro bezpečné používání mobilních zařízení.
b) Pravidla a postupy pro zajištění bezpečnosti zařízení, kterými orgán a osoba uvedená v § 3 písm. c) a d) zákona nedisponuje.

13. Politika poskytování a nabývání licencí programového vybavení a informací
[§ 5 odst. 1 písm. m), § 5 odst. 2 písm. j)]
a) Pravidla a postupy nasazení programového vybavení a jeho evidence.
b) Pravidla a postupy pro kontrolu dodržování licenčních podmínek.

14. Politika dlouhodobého ukládání a archivace informací
[§ 5 odst. 1 písm. n)]
a) Pravidla a postupy archivace dokumentů a záznamů.
b) Ochrana archivovaných dokumentů a záznamů.
c) Politika přístupu k archivovaným dokumentům a záznamům.

15. Politika ochrany osobních údajů
[§ 5 odst. 1 písm. o), § 5 odst. 2 písm. k)]
a) Charakteristika zpracovávaných osobních údajů.
b) Popis přijatých a provedených organizačních opatření pro ochranu osobních údajů.
c) Popis přijatých a provedených technických opatření pro ochranu osobních údajů.

16. Politika fyzické bezpečnosti
[§ 5 odst. 1 písm. p)]
a) Pravidla pro ochranu objektů.
b) Pravidla pro kontrolu vstupu osob.
c) Pravidla pro ochranu zařízení.
d) Detekce narušení fyzické bezpečnosti.

17. Politika bezpečnosti komunikační sítě
[§ 5 odst. 1 písm. q)]
a) Pravidla a postupy pro zajištění bezpečnosti sítě.
b) Určení práv a povinností za bezpečný provoz sítě.
c) Pravidla a postupy pro řízení přístupů v rámci sítě.
d) Pravidla a postupy pro ochranu vzdáleného přístupu k síti.
e) Pravidla a postupy pro monitorování sítě a vyhodnocování provozních záznamů.

18. Politika ochrany před škodlivým kódem
[§ 5 odst. 1 písm. r), § 5 odst. 2 písm. m)]
a) Pravidla a postupy pro ochranu komunikace mezi vnitřní a vnější sítí.
b) Pravidla a postupy pro ochranu serverů a sdílených datových úložišť.
c) Pravidla a postupy pro ochranu pracovních stanic.

19. Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí
[§ 5 odst. 1 písm. s), § 5 odst. 2 písm. n)]
a) Pravidla a postupy nasazení nástroje pro detekci kybernetických bezpečnostních událostí.

b) Provozní postupy pro vyhodnocování a reagování na detekované kybernetické bezpečnostní události.
c) Pravidla a postupy pro optimalizaci nastavení nástroje pro detekci kybernetických bezpečnostních událostí.

20. Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí

[§ 5 odst. 1 písm. t)]
a) Pravidla a postupy pro evidenci a vyhodnocení kybernetických bezpečnostních událostí.
b) Pravidla a postupy pravidelné aktualizace pravidel pro vyhodnocení kybernetických bezpečnostních událostí.
c) Pravidla a postupy pro optimální nastavení bezpečnostních vlastností nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí.

21. Politika bezpečného používání kryptografické ochrany

[§ 5 odst. 1 písm. u), § 5 odst. 2 písm. 1)]
a) Úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu.
b) Pravidla kryptografické ochrany informací
    1. při přenosu po komunikačních sítích,
    2. při uložení na mobilní zařízení nebo vyměnitelný technický nosič dat,
c) Systém správy klíčů.

B. Další dokumentace

1. Zpráva z auditu kybernetické bezpečnosti

[§ 28 odst. 1 písm. b)]
a) Cíle auditu kybernetické bezpečnosti.
b) Předmět auditu kybernetické bezpečnosti.
c) Kritéria auditu kybernetické bezpečnosti.
d) Identifikování týmu auditorů a osob, které se auditu kybernetické bezpečnosti zúčastnily.
e) Datum a místo, kde byly prováděny činnosti při auditu kybernetické bezpečnosti.
f) Zjištění z auditu kybernetické bezpečnosti.
g) Závěry auditu kybernetické bezpečnosti.

2. Zpráva z přezkoumání systému řízení bezpečnosti informací

[§ 28 odst. 1 písm. c)]
a) Vyhodnocení opatření z předchozího přezkoumání systému řízení bezpečnosti informací,
b) Identifikace změn a okolností, které mohou mít vliv na systém řízení bezpečnosti informací.
c) Zpětná vazba o výkonnosti řízení bezpečnosti informací
    1. neshody a nápravná opatření,
    2. výsledky monitorování a měření,
    3. výsledky auditu,
    4. naplnění cílů bezpečnosti,
d) Výsledky hodnocení rizik a stav plánu zvládání rizik.
e) Identifikace možností pro neustálé zlepšování.
d) Doporučení potřebných rozhodnutí, stanovení opatření a osob zajišťujících výkon jednotlivých činností.

3. Metodika pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik

[§ 28 odst. 1 písm. d), § 28 odst. 2 písm. b)]
a) Určení stupnice pro hodnocení primárních aktiv
    1. určení stupnice pro hodnocení úrovní důvěrnosti aktiv,
    2. určení stupnice pro hodnocení úrovní integrity aktiv,

3. určení stupnice pro hodnocení úrovní dostupnosti aktiv.

b) Určení stupnice pro hodnocení rizik

1. určení stupnice pro hodnocení úrovní dopadu,
2. určení stupnice pro hodnocení úrovní hrozby,
3. určení stupnice pro hodnocení úrovní zranitelnosti,
4. určení stupnice pro hodnocení úrovní rizik,

c) Metody a přístupy pro zvládání rizik.

d) Způsoby schvalování přijatelných rizik.

4. Zpráva o hodnocení aktiv a rizik

[§ 28 odst. 1 písm. e), § 28 odst. 2 písm. c)]

a) Přehled primárních aktiv

1. identifikace a popis primárních aktiv,
2. určení garantů primárních aktiv,
3. hodnocení primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti.

b) Přehled podpůrných aktiv (neplatí pro orgány a osoby uvedené v § 3 písm. e) zákona)

1. identifikace a popis podpůrných aktiv,
2. určení garantů podpůrných aktiv,
3. určení vazeb mezi primárními a podpůrnými aktivy,

c) Identifikování a hodnocení rizik

1. posouzení možných dopadů na aktiva,
2. hodnocení existujících hrozeb,
3. hodnocení existujících zranitelností, hodnocení existujících opatření,
4. stanovení úrovně rizika, porovnání této úrovně s kritérii pro přijatelnost rizik,
5. určení a schválení přijatelných rizik.

d) Zvládání rizik

1. návrh způsobu zvládání rizik,
2. návrh opatření a jejich realizace.

5. Prohlášení o aplikovatelnosti

[§ 28 odst. 1 písm. f), § 28 odst. 2 písm. d)]

a) Přehled vybraných bezpečnostních opatření včetně zdůvodnění jejich výběru a jejich vazby na identifikovaná rizika.

b) Přehled zavedených bezpečnostních opatření.

6. Plán zvládání rizik

[§ 28 odst. 1 písm. g), § 28 odst. 2 písm. e)]

a) Obsah a cíle vybraných bezpečnostních opatření pro zvládání rizik.

b) Potřebné zdroje pro jednotlivá bezpečnostní opatření pro zvládání rizik.

c) Osoby zajišťující jednotlivá bezpečnostní opatření pro zvládání rizik.

d) Termíny zavedení jednotlivých bezpečnostních opatření pro zvládání rizik.

e) Způsoby hodnocení úspěšnosti zavedení jednotlivých bezpečnostních opatření pro zvládání rizik.

7. Plán rozvoje bezpečnostního povědomí

[§ 28 odst. 1 písm. h), § 28 odst. 2 písm. f)]

a) Obsah a termíny poučení uživatelů.

b) Obsah a termíny poučení garantů aktiv (neplatí pro orgány a osoby uvedené v § 3 písm. e) zákona).

c) Obsah a termíny poučení administrátorů (neplatí pro orgány a osoby uvedené v § 3 písm. e) zákona).

d) Obsah a termíny poučení dalších osob zastávajících bezpečnostní role.

e) Obsah a termíny poučení nových zaměstnanců.

f) Formy a způsoby hodnocení plánu.

8. Zvládání kybernetických bezpečnostních incidentů

[§ 28 odst. 1 písm. i), § 28 odst. 2 písm. g)]

a) Definování kategorií kybernetického bezpečnostního incidentu.

b) Pravidla a postupy pro evidenci a zvládání jednotlivých kategorií kybernetických bezpečnostních incidentů.

c) Pravidla a postupy testování systému zvládání kybernetických bezpečnostních incidentů.

d) Pravidla a postupy pro vyhodnocení kybernetických bezpečnostních incidentů a pro zlepšování kybernetické bezpečnosti.

9. Strategie řízení kontinuity činností

[§ 28 odst. 1 písm. j), § 28 odst. 2 písm. h)]

a) Práva a povinnosti zúčastněných osob.

b) Cíle řízení kontinuity činností

1. minimální úroveň poskytovaných služeb,
2. doba obnovení chodu,
3. bod obnovení chodu.

c) Strategie řízení kontinuity činností pro naplnění cílů kontinuity.

d) Způsoby hodnocení dopadů kybernetických bezpečnostních incidentů na kontinuitu a posuzování souvisejících rizik.

e) Určení a obsah potřebných plánů kontinuity.

f) Postupy pro realizaci opatření vydaných Národním bezpečnostním úřadem.

10. Přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků

[§ 28 odst. 1 písm. k), § 28 odst. 2 písm. i)]

a) Přehled obecně závazných právních předpisů.

b) Přehled vnitřních předpisů a jiných předpisů.

c) Přehled smluvních závazků.

IV. Archiv

Pro archivaci již neplatných verzí dokumentů

Rekonstrukce a modernizace webových stránek Czech POINT

Zadavatel žádá o rekonstrukci a modernizaci webových stránek http://www.czechpoint.cz, včetně redakčního systému, podle níže uvedené specifikace. Údržbu těchto nových stránek bude provádět dodavatel podle odst. 2.7. Smlouvy.

Smluvní strany budou povinny poskytnout si navzájem veškerou součinnost, která se v průběhu plnění projeví jako potřebná. Předání a převzetí plnění bude potvrzeno předávacím protokolem podepsaným pověřenými zástupci obou smluvních stran. Vytvoření nových stránek je požadováno realizovat nejpozději do 30. 6. 2016.

1. Webové stránky a komunikační rozhraní domény http://www.czechpoint.cz

Komunikační rozhraní webových stránek bude napojeno na vybrané informační systémy ve správě Ministerstva vnitra. Komunikační rozhraní zabezpečí sdílení vybraných dat a jejich možnou prezentaci na webových stránkách např. v podobě statistik, či mapových výstupů.

Grafický návrh webových stránek bude zpracován v souladu s Logo manuálem projektu Czech POINT a Ministerstva vnitra. Webová prezentace včetně grafiky bude odpovídat podmínkám Blind friendly web. Stránky budou vytvořeny dle závazných pravidel, která určují, jak by měla být webová prezentace vytvořena tak, aby byla validní. Stránky budou vytvořeny v souladu s vyhláškou č. 64/2008 Sb., o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením (vyhláška o přístupnosti). S ohledem na bezpečnost bude dodržena minimálně metodika OWASP pro bezpečné webové prezentace (www.owasp.org), zejména s ohledem na OWASP Top 10 Rizik. Webová prezentace musí splňovat standardy W3C.

Pravidla, která bude vytvořené dílo dodržovat:

- Každý netextový prvek nesoucí významové sdělení musí mít svou textovou alternativu. Taktéž informace sdělované pomocí skriptů, appletů, obrázků a obdobných doplňků musí být dostupné bez kteréhokoliv z těchto doplňků na straně uživatele. Barvy prostředí musí být dostatečně kontrastní.
- Pro určení velkosti písma nesmí být použity absolutní jednotky a předpisy určující typ písma musí obsahovat celou rodinu písem.
- Obsah webové stránky musí řídit uživatel, obsah stránky se mění, pouze pokud uživatel aktivuje určitý prvek. Webová stránka bez přímého příkazu nesmí manipulovat uživatelským prostředím, pokud na to není uživatel výslovně upozorněn.
- Nová okna se otevírají jen v odůvodněných případech a uživatel je na to předem upozorněn. Obsah ani kód webové stránky nepředpokládá ani nevyžaduje konkrétní způsob použití ani konkrétní výstupní či ovládací zařízení.

Stránky musí být koncipovány tak, aby uživatele vždy co nejjednodušším způsobem dovedly k cíli. Navigace musí být přehledná, z každé stránky se uživatel musí jednoduše dostat na titulní stránku. Stránky musí obsahovat drobečkovou navigaci.

V hlavní sekci budou uveřejněny informace pro koncové uživatele, kteří by zde měli bez problémů nalézt požadované informace. Celá tato část webových stránek by měla být přístupná i pro osoby zrakově postižené.

Struktura webové prezentace musí být členěna dle požadavků hlavních cílových uživatelů. Detailní zpracování struktury webové prezentace bude zpracováno ve spolupráci s dodavatelem na základě základní analýzy požadavků cílových skupin.

Stránky bude možné zobrazovat také na mobilních zařízeních (smartphony a tablety). Navržené rozhraní musí být přehledné a uživateli musí umožnit jednoduchý a intuitivní pohyb včetně vyhledávání předmětů dle jednoduše nastavitelných kritérií.

Webová aplikace bude umožňovat spuštění více jazykových mutací, stránky budou obsahovat českou a anglickou jazykovou mutaci. Webová prezentace bude umožňovat fulltextové vyhledávání.

Na webové prezentaci budou zveřejněny převážně statické texty jako samotný obsah stránek včetně dokumentů ke stažení. Některé zveřejňované informace však budou načítány dynamicky z interních i externích datových zdrojů, např. statistiky typů podání, mapová prezentace, ale i případné ankety.

Webová prezentace musí být optimalizovaná pro běžné internetové prohlížeče (IE, Mozilla, Chrome, Safari).

2. Redakční systém

Redakční systém bude zabezpečovat editaci obsahové náplně webové prezentace a zároveň bude zajišťovat základní statistiky provozu webové prezentace. Redakční systém bude mít možnost diferencovaného uživatelského přístupu a s možností workflow schvalování textů k uveřejnění. Struktura webové prezentace bude členěna na základě definice cílových skupin v součinnosti se zadavatelem. Dodavatel zároveň dodá uživatelskou dokumentaci k redakčnímu systému.

Redakční systém musí být přístupný z prostředí internetu zabezpečenou komunikací. Redakční systém musí poskytovat kompletní portálové služby, potřebné pro vytvoření jednotného prostředí pro personalizovaný přístup k obsahu webové prezentace a k integrovaným aplikacím a funkcím.

Funkční požadavky:

- Autorizace a autentizace uživatele.
- Kompletní správa struktury webu s neomezenou hloubkou stromové struktury.
- Vytváření a editace článků pomocí komfortního WYSIWYG editoru.
- Schvalovací workflow článků (indikace stavu – schválené, upravené, publikované, archivované, apod.).
- Ruční určení doby platnosti článků.
- Podpora vytváření verzí článků a jejich archivace.
- Konfigurovatelná archivace článků (nastavení dne archivace).
- Tagování článků, možnost přidání neomezeného počtu tagů, správa tagů (editace, slučování), výpisy článků dle tagů a jejich kombinace.
- Možnost opatřit články vlastními metadaty.
- Možnost tvorby dynamicky načítaného obsahu z externích datových zdrojů.
- Personalizace obsahu.
- Možnost vkládání obrázků ve formátech JPG, PNG, GIF (včetně animovaného).
- Možnost vkládání video souborů ve standardních formátech.
- Možnost vkládání audio souborů ve standardních formátech.
- Možnost hromadného nahrávání souborů, včetně adresářů a podadresářů, přes webové rozhraní, bez nutnosti instalovat další podpůrné programy.
- Možnost náhledu na článek před publikací.
- Možnost fulltextového vyhledávání v článcích včetně příloh.
- Systém musí podporovat více jazykových mutací, včetně vyhledávání a umožňovat vytváření různých struktur pro jednotlivé jazykové mutace.
- Automatické generování sitemap.
- Automatické generování RSS dle nastavení správce systému.
- Možnost propojení se sociálními sítěmi.
- Možnost zasílání odkazů na článek e-mailem.
- Možnosti tisku článků.

- Statistiky činnosti uživatelů.
- Umožnění správy vícero webových prezentací (cílových webů).

Další požadované aplikace redakčního systému:

- Ankety s možností zadávání více otázek k jedné anketě.
- Diskuze k článkům, i samostatně stojící i s možností moderování.
- Notifikace nových článků na e-mail uživatelům, kteří si přejí být tímto způsobem informováni.
- Aktuality, možnost vytváření aktualit ze článků.
- Kalendář akcí.
- Podpora začlenění E-shop.
- Vytváření webových formulářů přímo správcem systému, ukládání dat zaslaných uživateli do databáze, možnost exportu do CSV.
- Nástroje pro monitoring a statistiky.
- Redakční systém bude napojen na Jednotný identitní prostor Czech POINTu.
- Umožnění sledování návštěvností webu bezplatným nástrojem Google analytics (vč. unikátního návštěvníka), (www.google.com/analytics).
- Umožnění exportování dat z toho webu.
- Nástroj na kontrolu aktuálnosti webových odkazů umístěných na webu.
- Umožnění vkládání iframe a portletů do šablon stránek.
- Umožnění vyhledávání v zobrazených a možnost filtrování údajů z externích databází přes webové služby (např. kontakty kontaktních míst veřejné správy).

Prvky webových stránek musí být v redakčním systému uloženy tak, aby byla umožněna jejich snadná úprava. Také musí umožňovat hromadné operace s články a strukturou, jako je její přesouvání, hromadné autorizace a podobně tak, aby byla maximálně zjednodušena práce šéfredaktora / správce webu. Prvky, které jsou využívány ve více stránkách, nesmí být v databázi duplicitně uloženy. Změna konkrétního prvku se musí projevit na všech stránkách, kde je tento prvek použit.

Redakční systém musí stránky generovat takovým způsobem, aby byly dobře čitelné pro vyhledávače, a tedy obsahovaly technickou optimalizaci pro vyhledávače SEO. Jedná se především o celkovou velikost stránky, správné použití meta tagů, keywords, description, title, robots a o správně generovanou sémantiku struktury dokumentu, použití nadpisů H1 až H6. Nezanedbatelným kritériem je taktéž velikost stránky, která by neměla přesáhnout 40kb. Redakční systém musí být schopen integračního a komunikačního rozhraní s externími datovými zdroji. Toto rozhraní musí umožňovat dynamické a automatické čerpání dat z Centrály Czech POINT (dostupnost cílových rejstříků, aktuální statistiky o provedených transakcích, mapová služba, kontakty kontaktních míst veřejné správy, aj.). Všechny dílčí části redakčního systému musí mít jednotné uživatelské prostředí pro uživatele a uživatelské skupiny.

Do redakčního systému budou přistupovat čtyři hlavní kategorie uživatelů s rozličnými právy přístupu, kterými jsou:

- správce systému (nejvyšší oprávnění v systému),
- schvalovatelé článků (šéfredaktoři),
- autoři a editoři článků,
- koncoví uživatelé (různé cílové skupiny uživatelů Czech POINT) nejnižší oprávnění v systému – pouze v roli přispěvatelů v diskuzích, anketách atp. prostřednictvím webové prezentace.

Každá z těchto skupin přistupuje k datům z různého úhlu pohledu, se specifickým oprávněním a se specifickým rozhraním pro zadávání a úpravu dat.

Správce systému:
Úroveň správce redakčního systému a databáze umožňuje spravovat nastavení oprávnění uživatelů, vytvářet a editovat obsah stránek, vytvářet a upravovat elektronické formuláře, vytvářet a upravovat šablony vzhledu webových stránek.

- kompletní správa redakčního systému
- vytváření workflow
- editace stromové struktury webu
- editace šablon webových stránek
- správa databáze souborů a obrázků
- kompletní správa systému, s přístupem ke všem statistickým výstupům včetně statistik z proxy serveru

Schvalovatelé článků:

- publikování a editace článků,
- možnost vrácení článku editorovi,
- přístup k veřejným i neveřejným dokumentům.

Autoři a editoři článků:

- tvorba a editace článků,
- přístup k veřejným i neveřejným dokumentům.

Koncoví uživatelé (široká veřejnost):

- přístup k hlavní prezentační vrstvě ze stolního PC nebo mobilních zařízení;
- možnost účasti v anketách