IL 024/10

D15053733

Dodatek č. 1 ke smlouvě o poskytování služeb ze dne 29.6.2010

Smluvní strany :

Poskytovatel:	**O2 Czech Republic a.s.**
Sídlo:	Za Brumlovkou 266/2 , 14022 Praha 4
IČ:	60193336
DIČ:	CZ 60193336
Zapsaná v obchodním rejstříku:	u Městského soudu v Praze, oddíl B, vložka 2322
Osoba oprávněná jednat jménem poskytovatele:	[redacted]

dále jen **poskytovatel**

a

Objednatel:	**Česká republika – Úřad průmyslového vlastnictví**
Sídlo:	Antonína Čermáka 2a, 160 68 Praha 6 – Bubeneč
Právní forma:	325 – organizační složka státu
IČ:	48135097
DIČ:	CZ48135097
Osoba oprávněná jednat jménem objednatele:	Ing. Luděk Churáček, ředitel ekonomického odboru

dále jen **objednatel**

Smluvní strany se dohodly na následujících úpravách smlouvy o poskytování služeb ze dne 29.6.2010 (dále jen „smlouva"):

I.
Úpravy smlouvy

Příloha č. 3 Celková bezpečnostní politika se nahrazuje aktualizovanou verzí dokumentu.

II.
Ostatní ustanovení

2.1 Všechna ostatní ustanovení smlouvy zůstávají nezměněna.
2.2 Dodatek ke smlouvě nabývá platnosti a účinnosti dnem podpisu.

V Praze dne 9.6.2015

za objednatele

[redacted]

Ing. Luděk Churáček
ředitel ekonomického odboru

V Praze dne

za poskytovatele

[redacted]

Celková bezpečnostní politika

Úřad průmyslového vlastnictví

verze 3.00

Verze	Popis	Provedl	Schválil	Platí od
1.00	Výchozí verze započetí implementace ISMS	XXXXX	Paclík	15.1.2007
1.00	Zapracovány připomínky z auditu	XXXXX	Paclík	9.4.2008
2.00	Opravená verze	XXXXX	Paclík	8.2.2010
3.00	Revize	XXXXX	Kratochvíl	8.4.2011
3.00	Revize	XXXXX	Paclík	26.3.2012
3.00	Revize	XXXXX	Paclík	20.3.2013
3.00	Revize	XXXXX	Paclík	4. 4. 2014

ID Dokumentu	UPV_Celk_Bezp_Pol	Verze	3.00
Autor	XXXXX	Datum revize	4.4.2014
Předkládá	XXXXX	Příští revize	4/2015
Schvaluje	Paclík	Platnost od	4.4.2014
Klasifikace	Neveřejné	Určeno pro	Úřad průmyslového vlastnictví
Počet výtisků	Neřízená elektronická kopie	Výtisk číslo	

Obsah

1. Úvodní ustanovení

1.1. Základní ustanovení a rozsah závaznosti

Cílem dokumentu Celková bezpečnostní politika ÚPV (dále též CBP ÚPV) je stanovit základní rámec řízení informační bezpečnosti. CBP ÚPV vymezuje základní pravomoci, odpovědnosti a definuje zásady systému managementu bezpečnosti informací Úřadu průmyslového vlastnictví (dále též ÚPV nebo Úřad).

Celková bezpečnostní politika ÚPV je zpracována v souladu s doporučeními normy pro řízení informační bezpečnosti ČSN ISO/IEC 17799:2006 „Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací" a normy pro zavádění a provoz ISMS ČSN ISO/IEC 27001:2006 „Informační technologie - Bezpečnostní techniky – Systémy managementu bezpečnosti informací - Požadavky".

Tato Celková bezpečnostní politika ÚPV je závazná pro ÚPV a pro zaměstnance, kteří jsou k ÚPV v pracovním poměru (dále jen „zaměstnanec"). Tato Celková bezpečnostní politika ÚPV se přiměřeně vztahuje i na fyzické osoby, které jsou v obdobném nebo jiném smluvním vztahu k Úřadu[1].

1.2. Definice základních pojmů

Aktivem se rozumí veškeré zpracovávané informace, veškerý hardware i software, dokumentace, tj. veškerý majetek, informace a činnosti, které mají pro ÚPV určitou hodnotu, jenž může být zmenšena působením určitých negativních vlivů.

Audit je systematický, nezávislý a dokumentovaný proces získávání důkazů z auditu a jeho objektivního hodnocení s cílem stanovit rozsah splnění kritérií auditu.

Bezpečnostní perimetr tvoří cokoliv, co vytváří bariéru, například zdi nebo vstupní turniket na karty. Fyzické ochrany může být dosaženo prostřednictvím řady fyzických bariér kolem prostor ÚPV a kolem prostředků zpracovávajících informace. Každá bariéra vytváří bezpečnostní perimetr a zajišťuje zvýšení ochrany.

Bezpečnostní opatření je praxe, postup nebo mechanismus, který snižuje riziko.

Bezpečnostní politika jsou pravidla, směrnice a praktiky, které rozhodují o tom, jak jsou aktiva včetně citlivých informací spravovány, chráněny a distribuovány uvnitř organizace a jejích systémů IT.

Bezpečnostní management ÚPV realizuje CBP ÚPV, sleduje dodržování bezpečnostních opatření ve všech oblastech informační bezpečnosti, navrhuje změny politiky, dohlíží na provedení změn, řeší bezpečnostní události a koordinuje školení zaměstnanců v oblasti informační bezpečnosti. Vede bezpečnostní dokumentaci ÚPV.

---

[1] Například na základě dohod o pracích konaných mimo pracovní poměr, mandátní smlouvy apod.

Bezpečnostní management zahrnuje Výbor pro integrovaný systém řízení a bezpečnostního manažera.

Dostupnost je vlastnost, že je něco na požádání přístupné a použitelné autorizovanou entitou.

Důvěrnost je vlastnost, že informace není dostupná nebo přístupná neautorizovaným jednotlivcům, entitám, nebo procesům.

Hrozba je potenciální příčina nežádoucího incidentu, který může mít za následek poškození systému nebo organizace.

Informace jsou výsledné, tj. vybrané či jinak zpracované údaje (data), prezentované ve formě snadno čitelné, pochopitelné a využitelné subjektem, jemuž jsou určeny. Mohou být v elektronické formě nebo napsaná (vytištěná) na papíře, vyřčená při jednání nebo zaznamenaná na jiném médiu

Informační aktiva tvoří zejména databáze a datové soubory, systémová dokumentace, uživatelské manuály, školicí manuály, provozní nebo podpůrné postupy, postupy obnovy, dohody o zajištění záložního provozu a archivní informace.

Informační bezpečnost jsou všechny aspekty související s definováním, dosažením a udržováním důvěrnosti, integrity, dostupnosti, individuální zodpovědnosti, autenticity a spolehlivosti.

Informační systém (IS) je identifikovatelný funkční celek zabezpečující cílevědomé a systematické shromažďování, zpracování, uchovávání a zpřístupňování informací. Informační systém integruje informační základnu (data), technické a programové vybavení, finanční prostředky, procedury a pracovníky.

Integrita je vlastnost, že data nebyla změněna nebo zničena neautorizovaným způsobem, nebo že systém vykonává svou zamýšlenou funkci nenarušeným způsobem, bez záměrné nebo náhodné neautorizované manipulace se systémem.

Klasifikace informací ÚPV definuje způsob, jakým se jednotlivým informacím přiřadí odpovídající klasifikační stupeň.

Kryptografický prostředek tvoří zařízení, předměty, programy nebo kryptografické postupy, včetně kryptografických klíčů, které zajišťují ochranu informací.

Monitorování sledování a vyhodnocování provozních událostí.

Odpovědnost je schopnost, kterou je určena odpovědnost za události.

Prostor ÚPV je místo, ve kterém se manipulují informace ÚPV, či ve kterém se nachází zařízení ÚPV.

Riziko vyjadřuje míru ohrožení aktiva, míru nebezpečí, že se uplatní hrozba a dojde k nežádoucímu výsledku vedoucímu ke vzniku škody.

Role je úloha, kterou byl zaměstnanec ÚPV pověřen v systému managementu bezpečnosti informací ÚPV.

Systém managementu bezpečnosti informací (dále též ISMS) je charakterizován jako soustava organizačních a technických opatření, která dostatečným způsobem eliminují rizika spojená se zachováním důvěrnosti, integrity a dostupnosti informací prostřednictvím pokrytí hrozeb doporučenými protiopatřeními dle norem ČSN ISO/IEC 27001:2006 „Informační technologie - Bezpečnostní techniky – systémy managementu bezpečnosti informací - Požadavky" a ČSN ISO/IEC 17799:2006 „Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací".

Vedoucím zaměstnancem se rozumí zaměstnanec ve smyslu § 74 zákona č. 6/2002 Sb., zákoník práce.

Zálohování je vytváření a uschovávání záložních kopií obchodních Informací k zajištění kontinuity činnosti pro případ ztráty zdrojů.

Zničení informace je stav informací ve kterém jsou informace nepoužitelné, bez ohledu na příčiny.

Zranitelnost je nedostatek, slabina, stav analyzované entity (aktiva, systému, objektu), kterého může být využito hrozbou pro uplatnění jejího nežádoucího vlivu. Tato veličina vyjadřuje, jak chráněné je aktivum vůči působení dané hrozby. Obvykle se vyjadřuje bez rozměru (např. malá, střední a velká), nebo jako pravděpodobnost, že hrozba způsobí škodu. Slabá místa mohou být využita k narušení zamýšleného chování IS. Zranitelnost se může projevit jak v oblasti důvěrnosti tak i integrity a dostupnosti. Využití zranitelnosti představuje hrozbu, se kterou souvisí odpovídající riziko.

1.3. Definice cíle informační bezpečnosti

Cílem informační bezpečnosti ÚPV je zajistit podporu činností Úřadu průmyslového vlastnictví při zachování dostupnosti, integrity a důvěrnosti zpracovávaných informací.

1.4. Definice strategie informační bezpečnosti

Informační bezpečnost je chápána jako celek složený z jednotlivých opatření organizační bezpečnosti, zajištění ochrany aktiv, personální a fyzické bezpečnosti a bezpečnosti informačních technologií pro zajištění dostupnosti, integrity a důvěrnosti informací ÚPV.

Základem prosazení informační bezpečnosti ÚPV je realizace a prosazení systému managementu bezpečnosti informací ve všech oblastech bezpečnosti.

Systém managementu bezpečnosti informací (dále též ISMS) je zaveden v souladu s normou ČSN ISO/IEC 27001:2006 a je zaveden pravidelně udržovaný systém správy záznamů ISMS.

Informační bezpečnost je ve všech součástech ÚPV prosazována v souladu s deklarovaným cílem a strategií a odpovídají za ni na všech úrovních vedoucí zaměstnanci.

Se zavedeným systémem řízení jsou seznámeni všichni zaměstnanci ÚPV.

K údržbě a zlepšování ISMS jsou prováděny pravidelné audity informační bezpečnosti a jsou přijímána nápravná a preventivní opatření.

1.5. Odpovědnost za informační bezpečnost

Odpovědnost za stav a řízení informační bezpečnosti ÚPV má předseda ÚPV.

Předseda ÚPV k prosazování opatření informační bezpečnosti zřizuje Výbor pro Integrovaný systém řízení ÚPV (dále jen Výbor pro ISŘ).

Za každodenní řešení problematiky informační bezpečnosti a šetření bezpečnostních incidentů je v rámci ÚPV odpovědný bezpečnostní manažer.

Odpovědnost za zavedení a dodržování bezpečnostních opatření a spolupráci při šetření bezpečnostních incidentů u jednotlivých součástí ÚPV nesou vedoucí zaměstnanci.

Odpovědnost za dodržování bezpečnostních opatření a ohlášení bezpečnostních incidentů nesou zaměstnanci ÚPV.

1.6. Regulatorní, legislativní a smluvní požadavky na informační bezpečnost

Systém řízení informační bezpečnosti ÚPV respektuje:

a) Požadavek zajistit podporu činností ÚPV při zachování dostupnosti, integrity a důvěrnosti zpracovávaných informací a

b) obecné právní požadavky.

ISMS je závislý na právních požadavcích, které jsou specifikovány ve Směrnici pro zajištění souladu s požadavky. Při změně výše uvedených, ale i dalších regulatorních norem je nutné provést revizi ISMS ÚPV.

1.7. Kritéria hodnocení rizik

Bezpečnostní opatření jsou vybrána na základě prováděného hodnocení rizik a požadavků zákonných a jiných norem.

Hodnocení rizik má za cíl určit možné hrozby, zranitelnosti a rizika hodnoceného systému, odhadnout ztráty, které mohou vzniknout působením hrozeb na informační aktiva zařazená do ISMS ÚPV. Hodnocení rizik se provádí s využitím analýzy rizik. Postup provádění analýzy rizik je podrobně popsán v dokumentu Metodika hodnocení rizik informační bezpečnosti.

Analýza rizik je aktualizována v periodě dvou let nebo v případě změn v informačních systémech a změn v požadavcích na informační bezpečnost.

1.8. Seznámení s CBP ÚPV

S dokumentem Celková bezpečnostní politika ÚPV bude seznámen každý vedoucí zaměstnanec ÚPV. Povinností vedoucích zaměstnanců je zajistit v přiměřené míře seznámení svých podřízených s tímto dokumentem.

Výklad této CBP ÚPV poskytuje bezpečnostní manažer ÚPV.

2. Zásady celkové bezpečnostní politiky

2.1. Prohlášení vedení ÚPV

Vedení ÚPV podporuje stanovené cíle a strategii bezpečnosti a ochrany informací ÚPV. Vyjádřením této podpory je schválení Celkové bezpečnostní politiky ÚPV.

ÚPV vyjadřuje touto CBP ÚPV svoji strategii trvalého zajišťování bezpečnosti a ochrany informací, jež jsou součástí řídících procesů ÚPV.

2.2. Systém managementu bezpečnosti informací ÚPV

Působnost systému managementu bezpečnosti informací (dále též ISMS) zahrnuje celý Úřad průmyslového vlastnictví, s důrazem na jím vykonávanou podporu veřejnoprávní ochrany průmyslového vlastnictví, zejména ve věcech patentů a ochranných známek, a s tím související provoz informačních a komunikačních technologií Úřadu.

ISMS je zavedeno na základě vymezení jeho působnosti, závěrů analýzy rizik, plánu řízení rizik a výběru vhodných opatření k zavedení informační bezpečnosti v rámci ÚPV, viz dokument Působnost systému managementu bezpečnosti informací.

2.3. Řídící dokumenty informační bezpečnosti ÚPV

Působnost ISMS upřesňuje rozsah systému řízení, vybraných lokalit a technologií.

Příručka ISŘ popisuje Integrovaný systém řízení ÚPV.

Metodika hodnocení rizik informační bezpečnosti ÚPV popisuje postup při analýze rizik systému řízení informační bezpečnosti a následný výběr opatření ke zvládání rizik.

Zpráva o hodnocení rizik definuje přístup k hodnocení rizik, identifikuje a hodnotí rizika.

Prohlášení o aplikovatelnosti obsahuje souhrnný přehled opatření aplikovaných v daném ISMS a případné důvody pro nezavedení nevhodných či nepřiměřených opatření.

Souhlas s navrhovanými zbytkovými riziky obsahuje přehled rizik přijatelných pro provoz Úřadu a souhlas vedení ÚPV se zavedením ISMS.

Plán zvládání rizik uvádí postup zavedení opatření včetně termínů a odpovědných osob, která jsou aplikována v systému řízení informační bezpečnosti ÚPV a uvedení opatření, která jsou tímto plánem redukována.

Celková bezpečnostní politika ÚPV definuje hlavní bezpečnostní cíle a stanovuje základní zásady informační bezpečnosti a určuje pravomoci a odpovědnosti pro její řízení.

Politika ISŘ s obsahem veřejné deklarace zavedení ISMS.

Bezpečnostní zásady CBP ÚPV jsou rozpracovány do směrnic dle jednotlivých oblastí informační bezpečnosti následovně:

a) **Směrnice řízení informační bezpečnosti ÚPV** definuje pravidla a postupy pro zajištění organizační bezpečnosti ÚPV.

b) **Směrnice klasifikace a řízení aktiv ÚPV** určuje způsob identifikace a ohodnocení aktiv. Směrnice dále určuje způsob klasifikace informací včetně klasifikačního schématu ÚPV a způsob manipulace s chráněnými informacemi ÚPV.

c) **Směrnice personální bezpečnosti ÚPV** definuje bezpečnostní pravidla a postupy pro oblast bezpečnosti lidských zdrojů ÚPV.

d) **Směrnice fyzické bezpečnosti a bezpečnosti prostředí ÚPV** definuje bezpečnostní pravidla a postupy pro oblast fyzické bezpečnosti a zabezpečení prostředí ÚPV.

e) **Směrnice správy SW a HW ÚPV** definuje základní rámec provozu prostředků pro zpracování informací ÚPV a služeb a procesů s tím souvisejících.

f) **Směrnice řízení přístupu uživatelů IT ÚPV** popisuje opatření zaměřená na ochranu a kontrolu přístupu k informacím, službám a procesům ÚPV.

g) **Směrnice správy bezpečnostních incidentů ÚPV** popisuje opatření k zajištění zvládání možného ohrožení bezpečnosti při zpracování informací ÚPV způsobem, který umožní včasnou nápravu.

h) **Směrnice pro řízení kontinuity činností ÚPV** definuje rámec řízení kontinuity činností ÚPV tvořený stanovením rolí, odpovědnosti, procesů a struktury dokumentace.

i) **Směrnice pro zajištění souladu s požadavky ÚPV** rozpracovává konkrétní postupy v oblasti zajištění shody přijímaných opatření s legislativou a bezpečnostními či technologickými postupy dle přijatých norem a standardů.

Záznamy informační bezpečnosti navazující na CBP ÚPV a bezpečnostní směrnice jednotlivých oblastí bezpečnosti, které jsou potřebné pro provoz ISMS. Záznamy jsou zpracovávány pro realizaci postupů a pravidel při každodenním prosazování informační bezpečnosti. Záznamy jsou uvedeny v jednotlivých směrnicích informační bezpečnosti.

Přezkoumání stavu informační bezpečnosti, které se zpracovává zpravidla při uzavření cyklu PDCA (dle ČSN ISO/IEC 27001:2006) s výsledkem nápravy nedostatků zjištěných při auditech ISMS.

3. Organizace bezpečnosti

3.1. Infrastruktura informační bezpečnosti

Cílem organizace bezpečnosti je stanovit rámec pro řízení, prosazování a kontrolu informační bezpečnosti v rámci ÚPV.

Bezpečnostní role vymezují odpovědnosti a pravomoci v rámci systému informační bezpečnosti ÚPV. Bezpečnostní role jsou přiřazeny k vybraným funkcím:

a) **řídící role** jsou přiřazeny vedoucím zaměstnancům ÚPV, kteří odpovídají za řízení informační bezpečnosti na své součásti ÚPV a za správu informačních aktiv,

b) **výkonné bezpečnostní role** jsou přiřazeny orgánům a osobám odpovědným za řízení informační bezpečnosti ÚPV; jedná se o Výbor pro ISŘ a bezpečnostní management,

c) **role řízení kontinuity činností** jsou přiřazeny orgánům a osobám odpovědným za správu řízení kontinuity činností ÚPV,

d) **role ve změnovém řízení** jsou přiřazeny osobám odpovědným za správu požadavků na IT ÚPV,

e) **uživatelské role** jsou přiřazeny zaměstnanci, který v rozsahu přidělených pravomocí využívá informace ÚPV.

Pro role uvedené pod písmeny a), b) a c) tohoto odstavce zpracovává bezpečnostní manažer písemné jmenování, které podepisuje předseda ÚPV.

Veškeré nově zaváděné technologie zpracovávající informace a soukromé prostředky zpracovávající pracovní informace podléhají schvalovacímu procesu a musí obsahovat řešení informační bezpečnosti. Za schválení odpovídají příslušní vedoucí zaměstnanci ÚPV.

Opatření organizace bezpečnosti zahrnují:

a) řízení informační bezpečnosti v rámci Úřadu s důrazem na přidělení odpovědností a koordinaci informační bezpečnosti, definování schvalovacího procesu prostředků IT, zajištění ochrany informací ve smlouvách s externími stranami a zajištění spolupráce s externími stranami v oblasti informační bezpečnosti;

b) řízení informační bezpečnosti s externími stranami včetně identifikace rizik spojených s jejich přístupem, zajištění bezpečného přístupu klientů a třetích stran k informacím ÚPV a zavázání těchto stran k dodržování požadavků ÚPV na zabezpečení informací.

4. Řízení a klasifikace aktiv

4.1. Odpovědnost za aktiva

Cílem identifikace a ohodnocení aktiv ÚPV je zabezpečit jejich přiměřenou ochranu.

Důležitá informační aktiva ÚPV jsou evidována v rámci ISŘ, je stanovena odpovědnost za jejich správu a je určen jejich garant. Za evidenci aktiva odpovídá jejich garant.

Garantem aktiva je zpravidla vedoucí zaměstnanec ÚPV, který nese za aktivum odpovědnost. Pro všechna důležitá aktiva musí garanti určovat přiměřená bezpečnostních opatření.

Uživatelem aktiva je součást ÚPV, jenž aktivum používá ke své práci. Uživatel aktiva je povinen dodržovat bezpečnostní opatření pro zacházení s aktivem stanovená garantem.

4.2. Klasifikace informací

Cílem klasifikace informací je zajištění přiměřenosti ochrany informačních aktiv ÚPV. Informace musí být klasifikovány na základě jejich potřebnosti a důležitosti pro zabezpečení obchodních činností ÚPV.

Každá informace, se kterou je nakládáno v rámci ÚPV má přiřazen klasifikační stupeň. Za obecné stanovení klasifikačního stupně k informačním aktivům odpovídá garant aktiva. Za přidělení konkrétního stupně klasifikace k informaci (v elektronické i listinné formě) odpovídá původce (autor, zhotovitel) informace.

Stupeň klasifikace ÚPV charakterizuje důležitost ochrany informace ÚPV a upřesňuje způsob, jak s ní lze nakládat.

Za účelem ochrany informací ÚPV jsou stanovena pravidla pro zacházení s informacemi ÚPV. Tato pravidla upřesňují zacházení s informacemi v souladu s jejich klasifikací v dokumentech, počítačových systémech, sítích, mobilních počítačích, hlasové komunikaci obecně, v multimédiích, v poštovním styku a při použití faxů.

Klasifikace informací se řídí příkazem předsedy ÚPV č. 3/2009.

5. Bezpečnost lidských zdrojů

5.1. Bezpečnost v popisu práce a při zajišťování lidských zdrojů

Cílem bezpečnosti lidských zdrojů je snížit riziko lidské chyby, krádeže, podvodu nebo zneužití prostředků ÚPV. Bezpečnost lidských zdrojů tvoří systém opatření, jejichž cílem je, aby se s chráněnými informacemi ÚPV seznamoval pouze zaměstnanec, který tyto informace potřebuje k výkonu své činnosti.

Přístup zaměstnanců k chráněným informacím vychází z jejich pracovního zařazení s důrazem na klasifikaci informací, s nimiž se na své funkci musí seznamovat. K upřesnění povinností zaměstnance v oblasti informační bezpečnosti jsou v rámci ÚPV definovány bezpečnostní role.

Opatření bezpečnosti lidských zdrojů jsou naplňovány v následujících fázích pracovního poměru:

a) **před uzavřením pracovním poměru** – musí být zajištěno, aby zaměstnanci ÚPV, byli prověřeni k manipulaci s informacemi ÚPV a znali své povinnosti při zajištění informační bezpečnosti ÚPV;

b) **v průběhu pracovního poměru** – musí být zajištěno, aby zaměstnanci ÚPV, byli řádně informováni o svých povinnostech v ISMS, byli motivováni k jejich plnění, byli řádně proškoleni a byli seznámeni s následky porušení požadavků na informační bezpečnost;

c) **při ukončení a změně pracovního poměru** – musí být zajištěno, aby zaměstnanci ÚPV, ukončili řádně a bezpečně ukončili svou činnost v ÚPV s důrazem na zrušení přístupových práv.

Všichni zaměstnanci ÚPV a zaměstnanci třetích stran, vyžaduje-li to jejich činnost, procházejí odpovídajícím a pravidelným školením o informační bezpečnosti ÚPV.

K prosazení zásad informační bezpečnosti do vědomí všech zaměstnanců probíhají v rámci ÚPV pravidelná školení.

6. Fyzická bezpečnost a bezpečnost prostředí

6.1. Bezpečnostní zóny

Cílem opatření fyzické bezpečnosti je předcházet neautorizovanému přístupu, poškození a zásahům do prostor a informací ÚPV.

Veškeré budovy, kanceláře, místnosti, prostory atd., v nichž jsou uchovávány chráněné informace ÚPV nebo v nichž se s nimi zachází, musí být zabezpečeny pomocí příslušných fyzických bezpečnostních opatření.

Bezpečnostní zóna je přesně definovaný stavebně ohraničený prostor uvnitř objektu, kde se zpracovávají nebo ukládají chráněné informace ÚPV. Opatření fyzické bezpečnosti použitá v bezpečnostních zónách jsou používána v závislosti na klasifikačním stupni chráněných informací, jejich významu a zpracovávaném množství. Bezpečnostní zónu tvoří samostatné zamykatelné kanceláře nebo několik místností, které obsahují uzamykatelné skříně, kontejnery a úschovné objekty.

Bezpečnostní zóny jsou chráněny přiměřenými kontrolami vstupu tak, aby bylo zajištěno, že osoba, která vstupuje do těchto prostor ÚPV, má ke vstupu oprávnění.

6.2. Bezpečnost zařízení

Zařízení ÚPV je libovolný technický, technologický nebo softwarový prostředek, který se používá pro zpracování, manipulaci či ukládání informací ÚPV. Zařízení ÚPV (včetně zařízení, která se používají mimo objekty ÚPV) jsou fyzicky chráněna proti bezpečnostním hrozbám a působení vnějších vlivů.

Zařízení zpracovávající informace ÚPV jsou umísťována tak, aby se minimalizovalo riziko působení vnějších vlivů a neautorizovaného přístupu.

Zařízení zpracovávající informace ÚPV jsou fyzicky chráněna v závislosti na stupni klasifikace informací jimi zpracovávaných. Zařízení ÚPV jsou též chráněna před výpadkem elektrického proudu nebo jinými anomáliemi napájení.

Pro správnou a bezpečnou funkci všech používaných zařízení a zajištění stálé dostupnosti a integrity činnosti ÚPV, je pravidelně a v souladu s pokyny výrobce prováděna údržba zařízení.

Oprava nebo likvidace zařízení, případně nosiče informací na nichž byly zpracovávány chráněné informace ÚPV musí být prováděna takovým způsobem, aby zaměstnancem, nebo zaměstnancem třetí stranou nebylo možné získat z tohoto zařízení informace, které na něm byly zpracovávány, a s nimiž tito zaměstnanci nejsou oprávněny se seznamovat.

7. Řízení komunikací a provozu

7.1. Provozní postupy a odpovědnosti

Řízení provozu tvoří soubor opatření spojených s řízením provozu informačních technologií ÚPV (dále též IT ÚPV). Provoz IT ÚPV se řídí postupy, požadavky a pravidly, která jsou řádně popsána v rámci dokumentace řízení provozu. Za prosazení bezpečnostních požadavků v oblasti řízení provozu IT ÚPV odpovídá ředitel odboru patentových informací.

V rámci IT ÚPV je zajištěno odpovídající oddělení vývojového, testovacího a provozního prostředí s cílem předcházet provozním problémům způsobovaným vývojovými a testovacími aktivitami. Jako součást oddělení těchto aktivit je definován proces uvedení změny do provozního prostředí.

7.2. Ochrana proti škodlivým a automaticky spouštěným programům

V rámci ÚPV je užíváno pouze schválené legální programové vybavení z důvěryhodných zdrojů. Užívání programového vybavení je kontrolováno.

Je zajištěno trvalé monitorování provozu důležitých částí IS ÚPV z hlediska aktivit potenciálních škodlivých programů. Možnost zavedení škodlivých programů do IS je minimalizována stanovením a prosazením vhodných postupů pro jejich odhalování a prevenci. Pro případ napadení škodlivým programem jsou stanoveny postupy a pravidla, se kterými jsou seznámeni všichni uživatelé IS ÚPV.

7.3. Správa provozního programového vybavení

Informace nezbytné pro ÚPV a pro provoz IS jsou, pro případ bezpečnostního incidentu, zajištěny uceleným systémem zálohování a obnovy ze záloh. Tento systém je navržen v souladu s potřebami řízení kontinuity činností ÚPV.

7.4. Postupy pro manipulaci s informacemi

Bezpečnost při zacházení s médii v oblastech správy vyměnitelných počítačových médií, likvidace nosičů dat, postupů pro manipulaci s informacemi a bezpečnost systémové dokumentace je řešena dle ustanovení CBP ÚPV pro oblast řízení a klasifikace aktiv a pro oblast fyzické bezpečnosti a bezpečnosti prostředí.

7.5. Výměna informací a programů

Výměna informací s externími subjekty je přesně specifikována včetně upřesnění bezpečnostních požadavků, schválena a ošetřena na úrovni smluvního vztahu.

Jsou stanoveny zásady, pravidla a postupy užívání elektronické pošty a jsou s nimi seznámeni všichni uživatelé IS tak, aby nedošlo k ohrožení provozu IS a zájmů ÚPV.

8. Řízení přístupu

8.1. Požadavky na řízení přístupu

Řízení přístupu je soustava opatření zaměřená na ochranu a kontrolu přístupu uživatelů k informacím a službám informačních systémů ÚPV. V rámci ÚPV je vytvořen, prověřován, udržován a prosazován systém řízení přístupu uživatelů IS ÚPV (dále též řízení přístupu), který se opírá o stanovené postupy a činnosti a o organizační strukturu danou stanovením rolí, pravomocí a odpovědností.

Řízení přístupu uživatelů ÚPV k informacím a službám IS ÚPV je prováděno na základě přidělených rolí a přístupových práv do jednotlivých IS a v souladu s klasifikací a řízením aktiv. Uživatelům IS ÚPV jsou přidělovány pouze přístupy nezbytné pro plnění jejich pracovních povinností v rámci ÚPV.

Přidělování rolí a konkrétních přístupových práv jednotlivým uživatelům je prováděno na základě žádostí nadřízených vedoucích zaměstnanců.

IT ÚPV je rozčleněno z hlediska řízení přístupu na jednotlivé IS ÚPV, které mají logicky ucelené a jednotné řízení přístupu, a u kterých jsou indikovány obdobné nároky z hlediska řízení přístupu.

Za stanovení politiky řízení přístupu a její prosazování v rámci jednotlivých IS ÚPV odpovídá ředitel odboru patentových informací. Za řízení přístupu v rámci jednotlivých IS odpovídají zaměstnanci pověření výkonem role bezpečnostní správce.

Proces řízení přístupu je rozpracován, popsán a dokumentován v rámci provozní dokumentace řízení přístupu, která zahrnuje řídící dokumentaci řízení přístupu IS, evidenční dokumentaci systému řízení přístupu ÚPV, dokumentaci přidělení, změny a odebrání přístupu a dokumentaci prověřování systému řízení přístupu ÚPV.

8.2. Řízení přístupu uživatelů

Jsou stanoveny, schváleny a prosazovány formální postupy registrace uživatelů IS ÚPV a správy přístupu zaměřené na přidělení, změnu a odebrání přístupu.

Jsou stanoveny postupy správy systému přístupu jednotlivých IS a postupy pravidelných kontrol shody aktuálního přidělení přístupů uživatelům IS ÚPV vůči evidenci přidělených přístupů.

Přidělování a užívání identifikačních a autentizačních informací a prostředků v rámci IS ÚPV se řídí stanovenými a schválenými postupy.

8.3. Odpovědnosti uživatelů

Všichni uživatelé jsou seznámeni se svými povinnostmi a s pravidly a postupy užívání přístupu k IS ÚPV s důrazem na používání uživatelských hesel a jiných autentizačních prostředků a ochranu neobsluhovaných aplikací, služeb a zařízení při přerušení nebo ukončení práce.

8.4. Používání síťových služeb

Řízení přístupu k síti je řešeno v souladu s obecným řízením přístupu k IS s tím, že jsou zdůrazněny specifické požadavky síťového prostředí. Důraz je kladen na:

a) pravidla pro přístup k sítím a síťovým službám, postupy pro autorizaci uživatelů sítí a síťových služeb a řídící a kontrolní mechanizmy a postupy k ochraně těchto přístupů,

b) technická, programová a organizační opatření na oddělení skupin informačních služeb, uživatelů a částí IS ÚPV do logických bezpečnostních domén.

9. Řízení přístupu k operačním systémům

Řízení přístupu k operačním systémům je řešeno v souladu s obecným řízením přístupu k IS s tím, že jsou zdůrazněna jejich specifika. Zohledněny jsou především požadavky:

a) realizace mechanismů pro identifikaci, autentizaci a blokování počítačových prostředků a uživatelů IS ÚPV a užívání bezpečných postupů přihlášení uživatelů,

b) užívání kryptografických mechanizmů a prostředků při autentizaci uživatelů přistupujících k chráněným informacím ÚPV,

c) prosazení mechanismů řízení kvality hesel a mechanismů zajišťujících bezpečnou a efektivní správu, výměnu a uložení hesel a jiných autentizačních informací nebo prostředků.

9.1. Řízení přístupu k aplikacím

Řízení přístupu k aplikacím je řešeno v souladu s obecným řízením přístupu k IS s důrazem na prosazení mechanizmů omezujících přístup k informacím a funkcím aplikací v souladu s požadavky na řízení přístupu, do aplikací ÚPV v době jejich vývoje.

9.2. Monitorování přístupu k systému a jeho použití

V rámci IS ÚPV jsou pro jednotlivé části stanoveny a prosazovány způsoby a postupy monitorování včetně rozsahu a ochrany pořizování auditních záznamů a jejich zálohování a archivace.

Auditní záznamy a záznamy zjištěných bezpečnostních událostí jsou pravidelně kontrolovány a vyhodnocovány.

Správnost časových údajů v auditních záznamech je zajištěna synchronizací času IS ÚPV.

9.3. Mobilní výpočetní prostředky a práce na dálku

Použití mobilních zařízení pro práci s IS ÚPV na dálku a vzdálený přístup k vnitřním IS ÚPV standardně nejsou možné. Výjimky podléhají posouzení a schválení ředitelem odboru patentových informací a bezpečnostním managementem a musí být řádně dokumentovány s ohledem na možná rizika.

10. Pořízení, vývoj a údržba informačních systémů

Cílem opatření vývoje a údržby IS ÚPV je prosadit informační bezpečnost do celého životního cyklu užívaných IS od fáze návrhu, vývoje, testování až po vlastní provoz a údržbu. Implementace součástí IS ÚPV a návrh jejich změn je v ÚPV spojen se stanovením vhodných bezpečnostních požadavků.

10.1. Bezpečnostní požadavky systémů

Provádění správy provozního prostředí zahrnuje provozování prověřeného a otestovaného programového vybavení, aktualizaci programového vybavení, vedení a vyhodnocování auditních záznamů, archivaci předešlých verzí programového vybavení a užívání nástrojů a postupů doporučených výrobcem (dodavatelem) programového vybavení.

10.2. Bezpečnost procesů vývoje a podpory

V rámci ÚPV podléhají veškeré změny informačních systémů, prostředí a aplikací postupům změnového řízení. V rámci změnového řízení je definován způsob provádění změn, vymezeny role, stanoven způsob dokumentace změn a popsány základní změnové činnosti.

Změna IS ÚPV je řízená úprava prostředí IS ÚPV oproti standardní dokumentované podobě, která mění chování IS jako celku nebo jeho částí. Pro potřeby změnového řízení je definována tzv. změnová oblast (vymezená část IS ÚPV a s ní související služby a procesy), která je relativně samostatná z hlediska řízení a realizace změnových řízení.

V rámci změnového řízení jsou vymezeny role správce změnové oblasti, který odpovídá za řádný průběh a dokumentaci prováděných změn a garant změny, který odpovídá za řádný průběh konkrétní změny.

Veškeré změny a provozní události jsou dokumentovány a zaznamenávány. Dokumentaci vývoje a údržby tvoří dokumentace změn, smluvní dokumentace a dokumentace kontrol.

11. Správa bezpečnostních incidentů

Cílem správy bezpečnostních incidentů je zajistit, aby incidenty a bezpečnostní slabiny byly komunikovány způsobem, který umožní včasnou nápravu s využitím formalizovaného a obecně známého postupu.

Bezpečnostní incident tvoří jedna nebo série nežádoucích nebo neočekávaných událostí informační bezpečnosti, které mají podstatnou šanci na kompromitaci podnikatelských operací a ohrožují informační bezpečnost.

Pro zajištění zpětné vazby při řešení bezpečnostních incidentů je prováděno jejich vyhodnocení. Vyhodnocení se využívá pro zpracování dodatečných nebo důkladnějších opatření, která by eliminovala frekvenci, závažnost a škody budoucích výskytů bezpečnostních incidentů. Hodnocení bezpečnostních incidentů je vzato v úvahu při revizi CBP ÚPV a plánů řízení kontinuity činností.

12. Řízení kontinuity činností

12.1. Aspekty řízení kontinuity činností

Cílem je zabránit přerušení činností ÚPV a chránit ÚPV před následky závažných chyb, katastrof a nepředvídatelných událostí nebo tyto následky minimalizovat. Důraz je položen na ochranu kritických procesů ÚPV souvisejících s hlavním informačním systémem ÚPV - Informačním systémem průmyslových práv SYP.

V rámci ÚPV je vytvořen, prověřován, udržován a prosazován proces řízení kontinuity činností ÚPV (dále jen řízení kontinuity), který se opírá o definované postupy, činnosti a organizační strukturu.

12.2. Kontinuita činností a analýza dopadů

ÚPV je z hlediska řízení kontinuity rozčleněna na jednotlivé oblasti řízení kontinuity ÚPV, které jsou buď částmi organizační struktury Úřadu, nebo částmi, u kterých jsou indikovány obdobné nároky z hlediska řízení kontinuity.

Za celkové řízení, koordinaci, údržbu a prosazování řízení kontinuity v rámci ÚPV odpovídá Koordinátor řízení kontinuity. Koordinátora řízení kontinuity jmenuje předseda ÚPV.

Proces řízení kontinuity je rozpracován, popsán a dokumentován v rámci dokumentace řízení kontinuity, která zahrnuje řídící dokumentaci (plán řízení kontinuity činností a seznam kontaktů), dokumentaci testů (zpráva o testu) a dokumentaci stavu ohrožení (deník stavu ohrožení a zpráva o stavu ohrožení).

12.3. Zvládání stavu ohrožení

Stavem ohrožení se rozumí stav v rámci ÚPV vyvolaný bezpečnostním incidentem, který vážným způsobem ohrožuje nebo narušuje informační bezpečnost ÚPV, a který je označen za stav ohrožení Hlavním koordinátorem.

Za zvládání stavu ohrožení v rámci ÚPV odpovídá Koordinátor řízení kontinuity, kterému v době stavu ohrožení přímo podléhají členové týmu kontinuity, případně další zaměstnanci.

12.4. Testování, udržování a přezkoumávání plánů kontinuity

Jednotlivé části systému řízení kontinuity a jejich vzájemný soulad jsou pravidelně testovány. Provádění testů nesmí ohrozit žádné činnosti ÚPV.

Systém řízení kontinuity je pravidelně revidován a aktualizován tak, aby byl zajištěn jeho soulad s potřebami ÚPV a byly odstraněny zjištěné nedostatky. Za údržbu systému řízení kontinuity odpovídá Koordinátor řízení kontinuity. Revize řízení kontinuity je provedena v případě potřeby, minimálně však 1x ročně.

13. Soulad s požadavky

13.1. Shoda s právními normami

Cílem je vyvarovat se porušení norem trestního nebo občanského práva, zákonných nebo smluvních povinností a bezpečnostních požadavků.

Pro zabezpečení informací ÚPV jsou jednoznačně definovány a zdokumentovány všechny relevantní zákonné a smluvní požadavky. ÚPV se řídí především zákony a nařízeními v oblastech obchodně právní, pracovně právní, občansko právní, trestní a správní.

Zvláštní pozornost věnují vedoucí zaměstnanci ÚPV dodržování ustanovení zákonů o ochraně duševního vlastnictví (především zákon č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským – autorský zákon), a ustanovením zákona č. 101/2000 Sb. o ochraně osobních údajů v platném znění.

Zajištění souladu s legislativou na ochranu osobních údajů dle zákona č.101/2000 Sb. v rámci ÚPV zajišťuje Odbor právní ÚPV. Odbor právní a bezpečnostní manažer poskytuje doporučení vedoucím zaměstnancům, uživatelům, třetím stranám a spolupracujícím organizacím k ochraně osobních údajů.

Prostředky pro zpracování informací ÚPV jsou provozovány pouze pro plnění služebních úkolů v rámci ÚPV. Jakékoliv použití těchto prostředků mimo pracovní rozsah, bez schválení vedoucím zaměstnancem, je považováno za zneužití těchto prostředků.

Použití služebního počítače pro neoprávněné účely je považováno za porušení pracovní kázně. Všichni uživatelé musí být obeznámeni s přesným rozsahem jejich přístupu.

13.2. Posouzení bezpečnostní politiky a technické shody

Cílem posouzení bezpečnostní politiky a technické shody je zajistit shodu systémů s CBP ÚPV a přijatými normami. Povinností všech vedoucích zaměstnanců ÚPV, je vést své podřízené k dodržování bezpečnostních zásad a opatření ISMS.

K zajištění plného souladu bezpečnostních zásad IB a technických komponent systémů ÚPV se všemi technickými normami, s doporučením výrobců, případně s jinými technickými požadavky, je prováděna pravidelná kontrola shody.

13.3. Hlediska auditu systému

Cílem zabezpečení auditu informační bezpečnosti a auditu provozovaných informačních systémů je zajistit ochranu provozních systémů, IS a auditních nástrojů v průběhu i po skončení auditu.

Auditní požadavky a činnosti zahrnující kontrolu informační bezpečnosti a IS ÚPV jsou plánovány a schváleny, tak aby se minimalizovalo riziko narušení činností ÚPV.

Záznamy o provedených auditech jsou ukládány odděleně od ostatní dokumentace.

14. Závěrečná ustanovení

14.1. Kontrola dodržování ustanovení CBP ÚPV

Předseda ÚPV a vedoucí zaměstnanci ÚPV zajistí kontrolu plnění povinností vyplývajících z ustanovení CBP ÚPV v mezích své působnosti.

Vedoucí zaměstnanci ÚPV zajistí, aby byli s CBP ÚPV seznámeni všichni zaměstnanci ÚPV.

Porušení zásad, postupů a pravidel informační bezpečnosti ÚPV zaměstnancem je považováno za porušením pracovní kázně a může být důvodem k rozvázání pracovního poměru.

14.2. Revize CBP ÚPV

Revize dokumentu Celková bezpečnostní politika je provedena v případě potřeby, minimálně však jednou ročně.

Za zpracování, prosazení, údržbu a revize dokumentu Celková bezpečnostní politika odpovídá bezpečnostní manažer ÚPV.

14.3. Audit CBP ÚPV

K prověření shody ustanovení dokumentu Celková bezpečnostní politika s reálným stavem v rámci ÚPV se provede 1x ročně audit.

Provádění interních i externích auditů se řídí vnitřními předpisy ÚPV.

14.4. Účinnost CBP ÚPV

Dokument Celková bezpečnostní politika schvaluje představitel vedení pro ISMS.

Celková bezpečnostní politika nabývá účinnosti a platnosti dnem vydání.