Dodatek č. 7 ke smlouvě o dílo ze dne 7.11.2001

Smluvní strany :

Zhotovitel:	**KOMTERM Čechy, s.r.o.**
Sídlo:	Bělehradská 15, 140 00 Praha
IČ:	28510011
DIČ:	CZ699001893
Zapsaná v obchodním rejstříku:	u Městského soudu v Praze, oddíl B, vložka 8117
Bankovní spojení:	[redacted]
Osoba oprávněná jednat jménem zhotovitele:	Jan Jelínek, jednatel

dále jen **zhotovitele**

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 dílo ze dne 7.11.2001 (dále jen „smlouva“):

I.
Úpravy smlouvy

1.1 Do článku 5. se doplňuje odstavec 5.12. v tomto znění:

„Zhotovitel se zavazuje při realizaci předmětu smlouvy dodržovat vnitřní pokyny a směrnice platné v budovách zadavatele, zejména pak Celkovou bezpečnostní politiku (příloha č. 1), Provozní řád budov užívaných Úřadem průmyslového vlastnictví (příloha č. 2) a dále pak povinnosti vztahující se k bezpečnosti a ochraně zdraví při práci a k ochraně životního prostředí definované v Manuálu pro dodavatele (příloha č. 3). Všechny výše uvedené dokumenty jsou nedílnou součástí této smlouvy jako její přílohy.“

1.2 Do smlouvy se doplňuje seznam příloh v tomto znění:

„Nedílnou součástí této smlouvy jsou následující přílohy:
1. Celková bezpečnostní politika
2. Provozní řád budov užívaných Úřadem průmyslového vlastnictví
3. Manuál pro dodavatele“

II.
Ostatní ustanovení

2.1 Všechna ostatní ustanovení smlouvy zůstávají nezměněna.
2.2 Dodatek ke smlouvě nabývá platnosti a účinnosti dnem 1.7.2016.

V Praze dne 22.6.2016

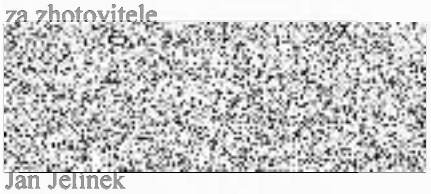
za objednatele

.....
Ing. Luděk Churáček
ředitel ekonomického odboru

Úřad průmyslového vlastnictví
Antonína Čermáka 2a
160 68 Praha 6 - Bubeneč
22

V Praze dne 22.6.2016

za zhotovitele



Jan Jelínek
jednatel

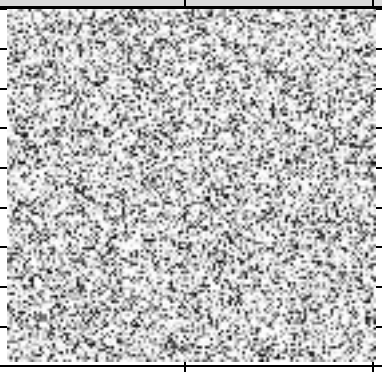
Komterm
ENERGETICKÉ SLUŽBY
KOMTERM Čechy, s.r.o.
Bělehradská 15, 140 00 Praha 4
IČ: [illegible]; DIČ: CZ699001893

Celková bezpečnostní politika

Úřad průmyslového vlastnictví

---

verze 5.00

Verze	Popis	Provedl	Schválil	Platí od
1.00	Výchozí verze započetí implementace ISMS			15.1.2007
1.00	Zapracovány připomínky z auditu			9.4.2008
2.00	Opravená verze			8.2.2010
3.00	Revize			8.4.2011
3.00	Revize			26.3.2012
3.00	Revize			20.3.2013
3.00	Revize			4.4.2014
4.00	Změna normy ČSN ISO/IEC 27001:2014			24.4.2015
5.00	Revize			7.3. 2016

ID Dokumentu	UPV_Celk_Bezp_Pol	**Verze**	5.00
Autor		**Datum revize**	7. 3. 2016
Předkládá		**Příští revize**	3/2017
Schvaluje		**Platnost od**	14. 3. 2016
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 ISMS ČSN ISO/IEC 27001:2014 „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 ve služebním/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].

1.1.1. Vnější kontext Úřadu

Úřad jako orgán veřejné správy je gestorem mezinárodních smluv na ochranu průmyslového vlastnictví, jimiž je Česká republika vázána. Do jeho působnosti náleží také podpora rozvoje a ochrany průmyslového vlastnictví.

Úřad spolupracuje se Světovou organizací duševního vlastnictví (WIPO), Evropským patentovým úřadem (EPO) a Úřad Evropské unie pro duševní vlastnictví (EUIPO), dále se podílí na činnosti Visegrádské skupiny.

1.1.2. Vnitřní kontext Úřadu

Úřad ve smyslu své zákonné působnosti rozhoduje o poskytování právní ochrany zejména na vynálezy, užitné vzory, průmyslové vzory, ochranné známky, vede rejstříky o těchto předmětech průmyslových práv, řeší případy sporné a odvolací. Vedle toho pečuje o zvyšování povědomí o přínosech a optimálních způsobech využívání systému ochrany průmyslového vlastnictví k podpoře podnikání a konkurenceschopnosti, výzkumu, vývoje a inovací.

Úřad tak v současné době plní a podílí se na plnění úkolů a opatření vyplývajících zejména z následujících dokumentů:

1. Národní program reforem (NPR) ČR 2012

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

2. Strategie mezinárodní konkurenceschopnosti ČR pro období let 2012 – 2020
3. Národní inovační strategie ČR usnesení č. 714 ze dne 27. září .

Úřad spravuje dva významné informační systémy dle vyhlášky 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích.

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. 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 zaměstnance.

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 je 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.

Představeným se rozumí zaměstnanec ve smyslu § 9 zákona č. 234/2014 Sb., služební zákon.

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 normy ČSN ISO/IEC 27001:2014 „Informační technologie - Bezpečnostní techniky – systémy managementu bezpečnosti informací - Požadavky“ .

Vedoucím zaměstnancem se rozumí zaměstnanec ve smyslu § 11 zákona č. 262/2006 Sb., zákoník práce.

Významný informační systém je systém splňující kritéria Vyhlášky 316/2014 Sb. Úřad spravuje dva VIS: ISDV a SYPP.

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.

Zákon o kybernetické bezpečnosti je zákon 181/2014 Sb., který definuje požadavky kybernetické bezpečnosti pro významné informační systémy Úřadu: ISDV a SYPP.

1.3. Definice cíle informační bezpečnosti

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

Systém informační a kybernetické bezpečnosti (dále též ISMS) je nedílnou součástí Integrovaného systému řízení (dále jen ISŘ) Úřadu průmyslového vlastnictví.

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 a kybernetické bezpečnosti ÚPV je realizace a prosazení systému managementu bezpečnosti informací ve všech oblastech činnosti Úřadu.

Systém managementu bezpečnosti informací (dále též ISMS) je v souladu s normou ČSN ISO/IEC 27001:2014 a je zaveden pravidelně udržovaný systém správy záznamů ISMS.

Systém managementu bezpečnosti informací (dále též ISMS) je v případě VIS podle vyhlášky 316/2014 Sb. rozšířen o povinnosti, které vyplývají ze zákona 181/2014 Sb. o kybernetické bezpečnosti.

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

Se zavedeným systémem řízení jsou seznámeni všichni zaměstnanci ÚPV.

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

1.5. Odpovědnost za informační bezpečnost

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

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

Za každodenní řešení problematiky informační a kybernetické 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 představení/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 a kybernetické 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 jeden krát za rok, nebo v případě změn v informačních systémech a změn v požadavcích na informační a kybernetickou bezpečnost.

1.8. Seznámení s CBP ÚPV

S dokumentem Celková bezpečnostní politika ÚPV bude seznámen každý představený/vedoucí zaměstnanec ÚPV. Povinností představených/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 a kybernetické bezpečnosti v rámci ÚPV, viz dokument Působnost systému managementu bezpečnosti informací.

2.3. Řídící dokumenty informační a kybernetické bezpečnosti ÚPV

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

Příručka ISŘ popisuje Integrovaný systém řízení ÚPV.

Metodika hodnocení rizik informační a kybernetické bezpečnosti ÚPV popisuje postup při analýze rizik systému řízení informační a kybernetické 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 a kybernetické bezpečnosti ÚPV a uvedení opatření, která jsou tímto plánem redukována.

Celková bezpečnostní politika ÚPV definuje hlavní bezpečnostní cíle a stanovuje základní zásady informační a kybernetické 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 a kybernetické bezpečnosti následovně:

a) **Směrnice řízení informační a kybernetické 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 a kybernetické 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 27001:2014) s výsledkem nápravy nedostatků zjištěných při auditech ISMS.

3. Proces řízení rizik

3.1. Politika managementu rizik Úřadu

Cílem managementu rizik je identifikace rizik v kontextu Úřadu, jejich posouzení a nastavení pravidel a opatření pro snižování jejich vlivů na činnost Úřadu.

3.2. Proces managementu rizik

Proces řízení rizik se skládá:

1) Určení kontextu Úřadu

2) Určení aktiv, procesů a jejich garantů

3) Procesu posuzování rizik

   - Identifikace rizik: plán hrozeb a jeho dopad na procesy a aktiva
   - Analýza rizik, vyhodnocení rizik
   - Plán zvládaní rizik zahrnující opatření na ošetření rizik

4) Pravidelné přezkoumání a vyhodnocení opatření

4. Politika organizace bezpečnosti

4.1. Infrastruktura informační bezpečnosti

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

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

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

b) **výkonné bezpečnostní role** jsou přiřazeny orgánům a osobám odpovědným za řízení informační a kybernetické bezpečnosti ÚPV dle zákona o kybernetické bezpečnosti 181/2014 Sb. a ČSN ISO/IEC 27001:2014; 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 představení/vedoucí zaměstnanci ÚPV.

Opatření organizace bezpečnosti zahrnují:

a) řízení informační a kybernetické bezpečnosti v rámci Úřadu s důrazem na přidělení odpovědností a koordinaci informační a kybernetické 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 a kybernetické 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.

5. Politika řízení a klasifikace aktiv

5.1. 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 představený/vedoucí zaměstnanec ÚPV, který nese za aktivum odpovědnost. Pro všechna důležitá aktiva musí garanti určovat přiměřená bezpečnostních opatření.

Správcem aktiva je zaměstnanec pověřený správou aktiva v rámci svých služebních/pracovních povinností.

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

5.2. 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.

6. Politika bezpečnosti lidských zdrojů

6.1. 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 služebního/pracovního zařazení s důrazem na klasifikaci informací, s nimiž se na své funkci musí seznamovat. K upřesnění povinností zaměstnance v oblasti informační a kybernetické bezpečnosti jsou v rámci ÚPV definovány bezpečnostní role.

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

a) **ihned po vzniku služebního/pracovním poměru** – musí být zajištěno, aby zaměstnanci ÚPV, byli prověřeni k manipulaci s informacemi ÚPV a znali své povinnosti při zajištění informační a kybernetické bezpečnosti ÚPV;

b) **v průběhu služebního/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 skončení a změně služebního/pracovního poměru** – musí být zajištěno, aby zaměstnanci ÚPV, skončili řádně a bezpečně svou činnost v ÚPV s důrazem na zrušení přístupových práv a vrácení přidělených aktiv.

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

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

7. Politika fyzické bezpečnosti a bezpečnosti prostředí

7.1. 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.

7.2. 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.

8. Politika řízení komunikací a provozu

8.1. 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.

8.2. 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.

8.3. 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.

8.4. 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.

8.5. 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.

9. Politika řízení přístupu

9.1. 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 služebních/pracovních povinností v rámci ÚPV.

Přidělování rolí a konkrétních přístupových práv jednotlivým uživatelům je prováděno na základě žádostí nadřízených představených/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.

9.2. 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.

9.3. 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.

9.4. 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.

10. 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.

10.1. 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.

10.2. 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.

10.3. 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.

11. 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.

11.1. 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.

11.2. 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.

12. Politika správy bezpečnostních incidentů

Bezpečnostní i kybernetický incident tvoří jedna nebo série nežádoucích neočekávaných událostí informační bezpečnosti, které mají podstatnou šanci ohrozit informační bezpečnost Úřadu.

Cílem správy bezpečnostních a kybernetických incidentů je zabránit přerušení nebo poškození činností Úřadu, nebo poškození dobrého jména Úřadu, umožnit včasnou nápravu s využitím formalizovaného a obecně známého postupu.

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

13. Politika řízení kontinuity činností

13.1. 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 SYPP a informačním systémem duševního vlastnictví ISDV.

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.

13.2. 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).

13.3. 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.

13.4. 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.

14. Soulad s požadavky

14.1. 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.

Úřad jako správce VIS se řídí , zákonem o kybernetické bezpečnosti 181/2014 Sb., Vyhlášky o kybernetické bezpečnosti 316/2014Sb.

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 představeným/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 představeným/vedoucím zaměstnancem, je považováno za zneužití těchto prostředků.

Použití služebního počítače pro neoprávněné účely je považováno za zaviněné porušení služební/pracovní kázně a je kárným proviněním. Všichni uživatelé musí být obeznámeni s přesným rozsahem jejich přístupu.

14.2. Posouzení bezpečnostní politiky a technické shody

Cílem posouzení bezpečnostní politiky a technické shody je zajistit shodu systémů s CBP ÚPV , zákonem o kybernetické bezpečnosti 181/2014 Sb., Vyhlášky o kybernetické bezpečnosti 316/2014Sb. a normy ČSN ISO/IEC 27001/2014. Povinností všech představených/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.

14.3. Hlediska auditu systému

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

Auditní požadavky a činnosti zahrnující kontrolu informační a kybernetické 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.

15. Závěrečná ustanovení

15.1. Kontrola dodržování ustanovení CBP ÚPV

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

Představení/vedoucí zaměstnanci ÚPV zajistí, aby byli s CBP ÚPV seznámeni všichni zaměstnanci ÚPV.

Porušení zásad, postupů a pravidel informační a kybernetické bezpečnosti ÚPV státním zaměstnancem je považováno za zaviněné porušení služební kázně a je kárným proviněním. Porušení zásad, postupů a pravidel informační a kybernetické bezpečnosti ÚPV zaměstnancem v pracovním poměru je považováno za porušení pracovní kázně a může být důvodem k rozvázání pracovního poměru.

15.2. 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.

15.3. 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.

15.4. Účinnost CBP ÚPV

Dokument Celková bezpečnostní politika schvaluje představitel vedení pro ISŘ.

Celková bezpečnostní politika nabývá účinnosti a platnosti dnem vydání.

PROVOZNÍ ŘÁD

budov užívaných Úřadem průmyslového vlastnictví

ve znění Příkazu č. 10 ze dne 11. 5. 2006, Příkazu č. 23 ze dne 18. 12. 2007, Příkazu č. 14 ze dne 26. 9. 2008, Příkazu č. 11 ze dne 20. 4. 2009, Příkazu č. 14 ze dne 1. 6. 2009, Příkazu č. 22 ze dne 14. 10. 2009, Příkazu č. 36 ze dne 24. 9. 2010, Příkazu č. 14 ze dne 15. 11. 2013, Příkazu č. 19 ze dne 20. 6. 2014, Příkazu č. 25 ze dne 8. 12. 2014, Příkazu č. 5 ze dne 13. 2. 2015, Služebního předpisu č. 30 ze dne 11. 5. 2016 a Služebního předpisu č. 32 ze dne 15. 6. 2016

Preambule

Provozní řád se vztahuje na budovy Úřadu průmyslového vlastnictví v ulici Antonína Čermáka 2a, Praha 6 a Ujkovice 66, Dolní Bousov.

Čl. 1
Přístup do budov

1. Budova skladu spisů Ujkovice 66 je trvale uzamčena. Vstup do areálu a do budovy je zabezpečován správcem objektu. Vstupující oprávněné osoby a dodavatelské firmy se zapisují do knihy příchodů a odchodů umístěné ve vstupní hale. Vstup je možný jen v pracovních dnech od 9:00 h do 13:00 h, případně podle potřeb provozu objektu. Budova skladu spisů Ujkovice 66 je nepřetržitě monitorována protipožárním systémem a elektronickým zabezpečovacím systémem napojeným na pult centrální ochrany.

2. Vstup do budovy v ulici Antonína Čermáka 2a, Praha 6 (dále jen „budova“) je zabezpečován nepřetržitou službou v recepci. Budova se otevírá v úřední dny v 6:00h a uzavírá ve 20:00 h. Ve dnech pracovního volna je budova uzavřena. Pro státní zaměstnance a zaměstnance Úřadu (dále jen „zaměstnanec“) a pracovníky cizích firem, kteří mají pracoviště v budově, je budova přístupná v úředních dnech od 6:00 h do 19:00 h. Výjimky povoluje ředitel ekonomického odboru nebo jeho zástupce na základě písemného zdůvodnění podepsaného příslušným vedoucím.
   Zaměstnanci Úřadu se v případě úrazu v budově ihned podrobí zjištění, zda nejsou pod vlivem alkoholu. V souladu s ustanovením § 106 zákona č. 262/2006 Sb. předseda Úřadu tímto určuje následující zaměstnance k provádění takového zjišťování: [redacted] Služba na recepci zajistí neprodlené vyrozumění výše uvedených zaměstnanců. O provedení zjištění bude pořízen písemný záznam a bezodkladně předán předsedovi Úřadu.

3. Zaměstnanci Úřadu a pracovníci dodavatelů, kteří mají pracoviště v budově, při průchodu recepcí označují svůj příchod a odchod pomocí elektronického identifikačního zařízení. Uvedená povinnost se nevztahuje na pracovníky, kteří zajišťují ostrahu budovy.

4. Pro veřejnost je budova přístupná v pondělí a ve středu od 8:00 h do 17:00 h, v úterý a ve čtvrtek od 8:00 h do 16:00 h a v pátek od 8:00 h do 14:30 h. Návštěvy se zapisují na recepci do knihy návštěv, kde je jim vydán badge „Návštěva“ po předložení platného občanského průkazu, případně cestovního pasu. Po budově se návštěvníci pohybují výhradně v doprovodu navštívené osoby nebo určeného zaměstnance.

5. Návštěvníci informačního střediska, podatelny a pokladny správních poplatků, jakož i uživatelé internetového pracoviště pro veřejnost a návštěvy přijímané ve vstupní hale Úřadu, se nezapisují v recepci do knihy návštěv. Rovněž se nezapisují ti návštěvníci studovny pro veřejnost, kteří zde hodlají pouze buď pořídit kopie přinesených písemností,

zakoupit odbornou literaturu, zaplatit poplatek za rešerši, nebo převzít připravenou rešerši.

6. Posluchači a vyučující Institutu průmyslově právní výchovy, lektoři jazykových kurzů pro zaměstnance Úřadu, posluchači a vyučující Metropolitní univerzity Praha, o.p.s. ve dnech výuky a zkoušek mají umožněn vstup do určených prostor Úřadu bez zápisu do knihy návštěv, a to na základě trvalého badge, který jim bude vydán na recepci Úřadu nebo Institutem průmyslově právní výchovy po předložení platného výkazu o studiu nebo občanského průkazu, případně cestovního pasu. V ostatní době jsou považováni za návštěvníky Úřadu.
   Důchodci, kteří v Úřadu pracovali do odchodu do důchodu, mají umožněn přístup do jídelny Úřadu bez zápisu do knihy návštěv, a to na základě trvalého badge, který jim bude vydán na recepci Úřadu po předložení platného občanského průkazu nebo cestovního pasu.
   Osoby, kterým byl vydán trvalý badge se pohybují v neveřejných prostorách Úřadu bez doprovodu.

7. Rovněž se nezapisují do knihy návštěv přihlášení účastníci seminářů, školení, exkurzí a pozvaní externí účastníci porad či obdobných jednání, konaných v prostorách přiléhajících ke vstupní hale, v případě souhlasu předsedy Úřadu nebo jeho zástupce, konaných i v jiných konkrétně určených prostorách v budově. Před konáním seminářů, školení, porad či pracovních jednání je organizátorem nebo gestorem vyhotoven, a v předstihu předán do recepce, seznam přítomných externích účastníků na prezenční listině.

8. Vstup a přítomnost osob dodavatelů zabezpečujících provoz budovy (opravy, údržba apod.) povoluje pro dobu od 7:00 h do 18:00 h v pracovních dnech věcně odpovědný vedoucí zaměstnanec; mimo tuto dobu ředitel ekonomického odboru. Dodavatelé se zapisují na recepci do knihy návštěv, kde je jim vydán badge „Dodavatel“ po předložení platného občanského průkazu, případně cestovního pasu. Dodavatelé se pohybují v neveřejných prostorách Úřadu bez doprovodu.

9. Cizinci mají vstup do budovy povolen jen v doprovodu zaměstnance, který jejich pobyt zabezpečuje. Tento zaměstnanec zajistí ve spolupráci se zaměstnancem recepce zápis v knize návštěv. Toto ustanovení se nevztahuje na vstup do podatelny, informačního střediska, pokladny správních poplatků a studovny pro veřejnost.

10. Neomezený přístup do budovy mají: předseda Úřadu, ředitel ekonomického odboru, vedoucí oddělení technických služeb, zástupce vedoucího oddělení technických služeb, ředitel odboru patentových informací a vedoucí oddělení analýz.

Čl. 2
Pohyb dopravních prostředků

1. Služební a určená soukromá osobní auta parkují v garáži v suterénu budovy. Ovladače od vrat garáže mají trvale řidiči a otevírání vrat zajistí v případě potřeby služba v recepci.

2. Služební nákladní auto a určená soukromá vozidla parkují na dvoře. Ovladače od vrat mají trvale řidiči a otevírání vrat v případě potřeby zajistí služba v recepci.

3. Dopravní prostředky dodavatelů vpouští do dvora služba v recepci po zápisu RZ do evidenční knihy.

4. Kromě doby od 6:00 h do 19:00 h v pracovních dnech je vjezd vozidel do areálu zakázán, případnou výjimku může povolit ředitel ekonomického odboru, případně předseda Úřadu. Služba v recepci o tom pořídí zápis do evidenční knihy.

Čl. 3
Ochrana majetku, služebních a osobních věcí, užívání kanceláří

1. Vstupy do všech kanceláří v budově jsou opatřeny zámkem a klíče jsou uloženy v recepci. Při příchodu si zaměstnanec vyzvedne klíč od místnosti, která mu je určena jako pracoviště. Při odchodu zaměstnanec odevzdá klíč službě v recepci. Pokud zaměstnanec vyzvedává klíče od jiné místnosti, zapíše toto služba do knihy s uvedením jména zaměstnance a časů, kdy byl klíč vydán a vrácen. Prázdné pracoviště musí být uzamčeno. Náhradní klíče od všech místností jsou uloženy u vedoucího oddělení technických služeb.

2. Zaměstnanci ukládají písemnosti obvykle do skříní a stolů na svém pracovišti. Cenné předměty svěřené jim organizací, razítka a služební peníze ukládají zaměstnanci na místě k tomu určeném příslušným vedoucím zaměstnancem.

3. Inventář pracoviště je zapsán do podepsaného místního seznamu na předepsaném formuláři.

4. Zaměstnanci jsou povinni šetrně zacházet s veškerým zařízením, inventářem budovy a kanceláří a chránit jej před poškozením, zneužitím nebo odcizením. Každý případ svévolného poškození a ztráty musí zaměstnanci neprodleně hlásit nadřízenému a vedoucímu oddělení technických služeb.

5. Zaměstnancům je zakázáno na pracovišti používat soukromé elektrické spotřebiče, které nemají platnou revizní zprávu uloženou v oddělení technických služeb. Elektrická topidla, která nejsou majetkem Úřadu, je zakázáno používat.

Čl. 4
Užívání jiných místností

1. V každém podlaží je určena místnost, v níž si zaměstnanec může připravit či ohřát nápoj nebo jednoduchý pokrm. Při zacházení s vybavením této místnosti jsou zaměstnanci povinni dodržovat zásady bezpečnosti a ochrany zdraví, bezpečnost v oblasti požární ochrany, chovat se hospodárně, udržovat čistotu a pořádek a počínat si tak, aby zařízení nebylo poškozováno a ostatní zaměstnanci nebyli při jeho používání nepřiměřeně omezováni.

2. Provozní prostory (kotelna, sklep, výtahové šachty, strojovny, střecha apod.) jsou pro osoby, které zde nevykonávají pracovní činnost, nepřístupné.

Čl. 5
Odchod z pracoviště

1. Po skončení pracovní doby je zaměstnanec kromě ledničky povinen vypnout veškeré elektrické spotřebiče včetně chladící jednotky. Okna musí být uzavřena. Zaměstnanec, který odchází z místnosti jako poslední, vše překontroluje, uzamkne místnost a klíč odevzdá v recepci.

Čl. 6
Zvláštní oprávnění a povinnosti

1. Klíče od vybraných místností (pokladna Úřadu, pokladna oddělení vstupního a poplatkového, místnost bezpečnostního ředitele, sklady, sál počítačů, knihovna odborové organizace, kantýna, jídelna, případně další místnosti) jsou trvale svěřeny pověřeným osobám a nevztahuje se na ně povinnost odevzdání v recepci. V recepci je uložen seznam těchto místností a pověřených osob. Klíče jsou uloženy v zalepených obálkách opatřených na přelepu podpisem pověřené osoby. Obálky s klíči jsou uloženy v trezoru v recepci pro případ havárie.

2. Osoby provádějící v budově úklid přebírají klíče od uklízeného úseku od služby v recepci proti podpisu v knize. Po ukončení úklidu klíče předávají službě v recepci. Tímto způsobem je také vedena kontrola evidence jejich příchodů a odchodů.

Čl. 7
Závěrečná ustanovení

1. Zrušuje se Provozní řád budov užívaných Úřadem průmyslového vlastnictví ze dne 25. května 2001.

2. Tento Provozní řád budov užívaných Úřadem průmyslového vlastnictví nabývá účinnosti dnem vydání.

předseda
Úřadu průmyslového vlastnictví

V Praze dne 20. dubna 2005

Manuál pro dodavatele

Schválil: J. Kratochvíl, předseda ÚPV
Dne: 12. 12. 2014

Verze	Popis	Provedl	Schválil	Platí od
1.00	Výchozí verze		Kratochvíl	21. 3. 2010
2.00	Změna pojmu „subdodavatel“ na „dodavatel“		Kratochvíl	20. 1. 2011
3.00	Revize		Kratochvíl	1. 1. 2015

Adresa prováděných prací: Antonína Čermáka 2a, 160 68 Praha 6 – Bubeneč

Stručná charakteristika prováděných prací: Komplexní služba pro soubor technologického zařízení vytápění v objektu sídla Úřadu průmyslového vlastnictví, garantující tepelný a časový režim vytápění, ohřevu TUV a dodávky tepla pro VZT.

Dodavatel: KOMTERM Čechy, s.r.o.

Termín realizace: Smlouva byla uzavřena na dobu neurčitou.

Odpovědná osoba ÚPV/kontakt: 

Odpovědná osoba dodavatele/kontakt: 

Další zastoupení/kontakt: (např. stavební dozor, koordinátor BOZP apod.)

Plánek objektu, kde jsou prováděny práce

Poznámka – pokud je to relevantní (podle rozsahu prací) zpracovat plánek objektu, vyznačit mj. také umístění: hlavního vypínače elektrické energie, hlavního uzávěru plynu, hlavního uzávěru vody, sběrných nádob odpadů.

Kontakty na složky IZS
(Integrovaný záchranný systém)

LINKA TÍSŇOVÉHO VOLÁNÍ : 112

HASIČI : 150

ZÁCHRANNÁ SLUŽBA : 155

POLICIE : 158

OKAMŽITĚ UPOZORNIT odpovědnou osobu ÚPV

VŠICHNI VEDOUCÍ PRACOVNÍCI JSOU ODPOVĚDNI ZA ZDRAVÍ A BEZPEČNOST SVÝCH ZAMĚSTNANCŮ VE SVÉ PRACOVNÍ OBLASTI.

Část 1 – BOZP a kvalita

Obecná ustanovení

Hlavní dodavatel musí informovat odpovědnou osobu ÚPV o počtu osob, které se budou pohybovat na místě provádění prací.

Každý dodavatel musí předem nahlásit, jaké energie a v jakém množství bude potřebovat pro své práce.

Každý dodavatel se musí přizpůsobit časový harmonogram prací podmínkám stanoveným ÚPV.

Každý dodavatel musí předem odpovědné osobě ÚPV, kolik místa bude potřebovat pro uskladnění svého materiálu v průběhu svých prací.

Každý dodavatel musí předem pro lepší koordinaci stanovit četnost svých dodávek na místo realizace prací. U zásobování do pater musí dodavatel předem sdělit způsob dopravy do pater.

Každý dodavatel odevzdá před započetím prací plán svých prací, aby bylo možné zajistit ze strany ÚPV účinnou synchronizaci všech dalších prací a činností ÚPV.

Každý dodavatel se zavazuje, že bude své práce koordinovat se všemi případnými ostatními dodavateli. Toto opatření umožní organizovat práce různých firem na jednom místě.

Každý dodavatel musí oznámit odpovědnému pracovníkovi ÚPV jakýkoli problém týkající se postupu prací.

Každý dodavatel musí po sobě zajistit úklid. Tříděný odpad se nutné bezpečně skladovat, a to podle doporučení ustanoveném v hlavní smlouvě. Pokud dodavatel není schopen své závazky splnit, zajistí odpovědný pracovník ÚPV provedení úklidových prácí na náklady dodavatele.

Hygienická a bezpečnostní pravidla

Každý dodavatel se zavazuje, že bude dodržovat hygienická a bezpečnostní pravidla, vztahující se k jeho pracím a stanovená v platné legislativě, dále pak zvláštní pravidla předepsaná ze strany ÚPV, jimž se musí povinně přizpůsobit.

Každý dodavatel zajišťuje bezpečnost svých vlastních zaměstnanců a všech dalších osob, které budou provádět jeho práce, a všech ostatních, kteří budou na jejich práci dohlížet a kontrolovat ji. Tyto osoby musí být před vstupem na místo provádění prací prokazatelně seznámeny s bezpečnostními pokyny, možnými nebezpečími apod. a musí být vybaveny příslušnými osobními ochrannými prostředky, úměrnými nebezpečím ohrožení jejich bezpečnosti a zdraví. Zařízení pro bezpečnost jednotlivce musí být ve shodě s platným nařízením. Bezpečnostní vybavení musí být schopna čelit případným rizikům**.**

Každý dodavatel je zodpovědný za jakékoli nehody nebo škody, které způsobí komukoli dalšímu, a to z důvodu chybného provádění svých prací nebo činností kteréhokoli svého pracovníka.

Je nutné dávat přednost kolektivní prevenci úrazů před individuální prevencí úrazů, např.: upřednostňovat sítě (pletiva) pod konstrukcí před pevnými či pojízdnými bezpečnostními popruhy každého pracovníka zvlášť.

Pracovní postupy

Každý dodavatel je povinen ověřit přiměřenost svých pracovních postupů vůči postupům, které předpokládají případné spolupracující firmy, zvláště co se týká na sebe navazujících prací.

Bezpečnostní pravidla

Každý dodavatel musí dbát na zachování bezpečnostních instalací a zařízení, umístěných na místě realizace prací. Pod žádnou záminkou nesmí dodavatel na staveništi jakkoli měnit nařízené bezpečnostní instalace ani ochranná opatření.

Identifikace a klasifikace rizik

Všichni dodavatelé budou odpovědným pracovníkem ÚPV, nebo jím pověřenou osobou seznámeni s ní zpracovaným registrem rizik, včetně souvisejících opatření, vedoucích k eliminaci těchto rizik
Ve vztahu k jím prováděným činnostem je každý dodavatel povinen zpracovat svůj registr rizik, včetně identifikace jejich závažnosti a souvisejících opatření, vedoucích k jejich eliminaci. Tento registr předá odpovědnému pracovníkovi ÚPV, nebo jím pověřené osobě.

Dodávky a skladování materiálu na stavbě

Každý dodavatel musí předem nahlásit odpovědnému pracovníkovi ÚPV, nebo jím pověřené osobě termíny, kdy požaduje zajištění vjezdu do objektu/na místo realizace prací z důvodu dodávky potřebného materiálu.
Předem je určen dostatečný a vhodný prostor ke skladování dovezeného materiálu.

Kvalita materiálu použitého na stavbě

Každý dodavatel se zavazuje, že u všech zařízení (jeřáby, výtahy, lešení, ochranná zábradlí nebo sítě/pletiva, elektrická zařízení apod.) a pomocných prostředků (např. zvedací, tlaková a elektrická zařízení), u kterých musí být podle příslušných předpisů prováděny revize, kontroly apod. budou tyto provedeny před zahájením jejich používání a v průběhu realizace prací musí být podle v předpisech stanovených intervalech obnovovány. Záznamy o těchto revizích, kontrolách atd. musí být k dispozici u zařízení, nebo u příslušného vedoucího pracovníka dodavatele. Za výše uvedené prostředky, dodané jinými firmami, bude zodpovědný příslušný dodavatel.

Každý dodavatel se zavazuje, že bude na místě prací manipulovat se všemi materiály pomocí normalizovaných nářadí a přístrojů, které budou v dobrém stavu.

Každý dodavatel musí průběžně dodávat svým zaměstnancům potřeby, nezbytné pro dodržování hygienických a bezpečnostních pravidel. Seznam těchto materiálů není omezen platnou legislativou.

Přístup k elektrickým rozvodům a dalším hlavním ovládacím prvkům

Otevíráním skříní, které obsahují obnažené vodiče pod napětím, jsou pověřeny pouze oprávněné osoby. Při realizaci díla musí být neustále zajištěn přístup ke všem hlavním ovládacím prvkům.

Manipulace se stroji

Obsluhu všech zařízení budou provádět pouze osoby, řádně pro tyto činnosti kvalifikované podle příslušných předpisů.

Přístup na místo realizace prací

Na místo realizace prací smí vstoupit pouze tyto oprávněné osoby:

Ze strany ÚPV: 

Ze strany dodavatele: 

Další pracovníci dodavatele (nebo cizí osoby, jejichž činnost na místě prací je vyžadována dodavatelem) smí vstoupit na místo prací **pouze se souhlasem odpovědného pracovníka ÚPV, nebo jím pověřené osoby a pouze v doprovodu oprávněné osoby dodavatele.** Odpovědný pracovník dodavatele odpovídá za prokazatelné seznámení této osoby s riziky BOZP a za její případné vybavení předepsanými OOPP.

Povinnosti zaměstnanců a zaměstnavatelů po zjištění pracovním úrazu

DEFINICE: "Pracovní úraz je úraz, který se stal při plnění pracovních povinností nebo v přímé souvislosti s ním."

***Postupovat v souladu s nařízením vlády č. 170/2014 Sb.,* o způsobu evidence úrazů, hlášení a zasílání záznamu o úrazu**

- zaměstnanec dodavatele je povinen bezodkladně ohlásit svůj pracovní úraz určenému zástupci ÚPV a bezprostřednímu nadřízenému svého zaměstnavatele (pokud je schopen) nebo pracovní úraz, jehož byl svědkem a spolupracovat při jeho vyšetření,
- zaměstnavatel (dodavatel) spolu se zástupcem ÚPV vyšetřit příčiny a okolnosti vzniku pracovního úrazu za účasti zaměstnance, pokud to zdravotní stav zaměstnance dovoluje,
- záznam o úrazu sepíše zaměstnavatel postiženého pracovníka (dodavatele) dle příslušného právního předpisu.
- zaměstnavatel (dodavatel) postiženého pracovníka zašle záznam o úrazu stanoveným orgánům a institucím dle příslušného právního předpisu,
- zaměstnavatel (dodavatel) musí stanovit potřebná opatření proti opakování pracovních úrazů.

ZÁZNAM O ÚRAZU

- ☐ smrtelném
- ☐ s hospitalizací delší než 5 dnů
- ☐ ostatním

Evidenční číslo úrazu [a]:
Evidenční číslo zaměstnavatele [b]:

A. Údaje o zaměstnavateli, u kterého je úrazem postižený zaměstnanec v základním pracovněprávním vztahu

1. IČO: Název zaměstnavatele a jeho sídlo (adresa):	2. Předmět podnikání (CZ-NACE), v jehož rámci k úrazu došlo:
	3. Místo, kde k úrazu došlo [c]:
	4. Bylo místo úrazu pravidelným pracovištěm úrazem postiženého zaměstnance? ☐ Ano ☐ NE

B. Údaje o zaměstnavateli, u kterého k úrazu došlo (pokud se nejedná o zaměstnavatele uvedeného v části A záznamu)

1. IČO: Název zaměstnavatele a jeho sídlo (adresa):	2. Předmět podnikání (CZ-NACE), v jejíž rámci k úrazu došlo:
	3. Místo, kde k úrazu došlo:

C. Údaje o úrazem postiženém zaměstnanci

1. Jméno, příjmení:	Pohlaví: ☐ Muž ☐ Žena
2. Datum narození:	3. Státní občanství:
4. Adresa pro doručování:	
5. Druh práce (CZ-ISCO):	6. Činnost, při které k úrazu došlo [d]:
7. Délka trvání základního pracovněprávního vztahu u zaměstnavatele Roků: Měsíců:	
8. Úrazem postižený je ☐ zaměstnanec v pracovním poměru ☐ zaměstnanec zaměstnaný na základě dohod o pracích konaných mimo pracovní poměr ☐ osoba vykonávající činnosti nebo poskytující služby mimo pracovněprávní vztahy (§ 12 zákona č. 309/2006 Sb.)	

9. Trvání pracovní neschopnosti následkem úrazu [c)]:		
Od:	do:	Celkem kalendářních dnů:

D. Údaje o úrazu

1. Datum úrazu: Hodina úrazu: Datum úmrtí úrazem postiženého zaměstnance:	2. Počet odpracovaných hodin bezprostředně před vznikem úrazu:
3. Druh zranění [f)]:	4. Zraněná část těla [g)]:
5. Počet zraněných osob celkem:	
6. Co bylo zdrojem úrazu? ☐ dopravní prostředek ☐ stroje a zařízení přenosná nebo mobilní ☐ materiál, břemena, předměty (pád, přiražení, odlétnutí, náraz, zavalení) ☐ pád na rovině, z výšky, do hloubky, propadnutí ☐ nástroj, přístroj, nářadí	☐ průmyslové škodliviny, chemické látky, biologické činitele ☐ horké látky a předměty, oheň a výbušniny ☐ stroje a zařízení stabilní ☐ lidé, zvířata nebo přírodní živly ☐ elektrická energie ☐ jiný blíže nespecifikovaný zdroj a)
7. Proč k úrazu došlo? (Příčiny) ☐ pro poruchu nebo vadný stav některého ze zdrojů úrazu ☐ pro špatné nebo nedostatečné vyhodnocení rizika ☐ pro závady na pracovišti	☐ pro nedostatečné osobní zajištění zaměstnance včetně osobních ochranných pracovních prostředků ☐ pro porušení předpisů vztahujících se k práci nebo pokynů zaměstnavatele úrazem postiženého zaměstnance ☐ pro nepředvídatelné riziko práce nebo selhání lidského činitele ☐ pro jiný, blíže nespecifikovaný důvod a)
8. Byla u úrazem postiženého zaměstnance provedena kontrola přítomnosti alkoholu nebo jiných návykových látek, a pokud ano, s jakým výsledkem? Ano: Ne: Výsledek:	

9. Popis úrazového děje, rozvedení popisu místa, příčin a okolností, za nichž došlo k úrazu.
(V případě potřeby přidejte další list).

a)

10. Uveďte, jaké předpisy byly v souvislosti s úrazem porušeny a kým, pokud bylo jejich porušení do doby odeslání záznamu zjištěno. *(V případě potřeby přidejte další list.)* [h)]

11. Opatření přijatá k zabránění opakování pracovního úrazu:

E. Vyjádření úrazem postiženého zaměstnance a svědků úrazu, případně dalších osob

Úrazem postižený zaměstnanec	..... Datum, jméno, příjmení a podpis
Svědci	..... Datum, jméno, příjmení a podpis

	..... Datum, jméno, příjmení a podpis ..... Datum, jméno, příjmení a podpis
Zástupce zaměstnanců pro bezpečnost a ochranu zdraví při práci [i)]	..... Datum, jméno, příjmení a podpis
Za odborovou organizaci [i)]	..... Datum, jméno, příjmení a podpis
Za zaměstnavatele [i)]	..... Datum, jméno, příjmení a podpis Pracovní zařazení:

[a)] Vyplní orgán inspekce práce, popřípadě orgán báňské správy.

[b)] Vyplní zaměstnavatel

[c)] Uvede se typ pracoviště, pracovní plochy nebo lokality, kde byl úrazem postižený zaměstnanec přítomen nebo pracoval těsně před úrazem, a kde došlo k úrazu, například průmyslová plocha, stavební plocha, zemědělská nebo lesní plocha, zdravotnické zařízení, terciální sféra – úřad.

[d)] Činností se rozumí hlavní typ práce s určitou délkou trvání, kterou postižený zaměstnanec vykonával v čase, kdy k úrazu došlo, například svařování plamenem. Nejedná se o konkrétní úkon, například zapálení hořáku při svařování plamenem.

[e)] Konec pracovní neschopnosti se vyplňuje pouze v případě, kdy byla pracovní neschopnost skutečně ukončena.

[f)] Do rámečku se uvede trojmístný číselný kód klasifikace zraněné části těla podle Přílohy č. 3 tohoto nařízení.

[g)] Do rámečku se uvede dvojmístný číselný kód klasifikace pro zraněnou část těla podle Přílohy č. 3 tohoto nařízení.

[h)] Porušení předpisů se týká jak předpisů právních, tak i ostatních a konkrétních pokynů k zajištění bezpečnosti a ochrany zdraví při práci, daných zaměstnanci vedoucími zaměstnanci, kteří jsou mu nadřízeni ve smyslu § 349 odst. 1 a 2 zákoníku práce. Předpisy se rozumí předpisy na ochranu života a zdraví, předpisy hygienické a protiepidemické, technické předpisy, technické dokumenty a technické normy, stavební předpisy, dopravní předpisy, předpisy o požární ochraně a předpisy o zacházení s hořlavinami, výbušninami, zbraněmi, radioaktivními látkami, chemickými látkami a chemickými přípravky a jinými látkami škodlivými zdraví, pokud upravují otázky týkající se ochrany života a zdraví.

[i)] V případě, že některá z osob, které záznam o úrazu podepisují, chce podat vyjádření, učiní tak na zvláštním listě, který se k záznamu o úrazu připojí.

ZÁZNAM O ÚRAZU – HLÁŠENÍ ZMĚN

Evidenční číslo úrazu [a)]
Evidenční číslo zaměstnavatele [b)]

Údaje o zaměstnavateli, který záznam o úraze odeslal

Název zaměstnavatele:	IČO:
	Adresa:

Údaje o úrazem postiženém zaměstnanci a o úrazu

Jméno a příjmení:	Datum úrazu:
Datum narození:	Místo, kde k úrazu došlo:

Hospitalizace úrazem postiženého zaměstnance přesáhla 5 kalendářních dnů:
☐ Ano ☐ Ne

C 8 - Trvání dočasné pracovní neschopnosti následkem úrazu:

Od: do: celkem kalendářních dnů:

D 1 – Úrazem postižený zaměstnanec na následky poškození zdraví při úrazu zemřel dne:

Jiné změny:

Úrazem postižený zaměstnanec	..... Datum, jméno, příjmení a podpis
Zástupce zaměstnanců pro bezpečnost a ochranu zdraví při práci	..... Datum, jméno, příjmení a podpis
Za odborovou organizaci	.....

	Datum, jméno, příjmení a podpis
Za zaměstnavatele:	..... Datum, jméno a podpis Pracovní zařazení:

[a)] Vyplní orgán inspekce práce, popřípadě orgán báňské správy.
[b)] Vyplní zaměstnavatel

Část 2 – Environment

Povinnosti dodavatele

Obecné povinnosti

Dodavatel má při své činnosti nebo v rozsahu své působnosti povinnost předcházet vzniku odpadů, omezovat jejich množství a nebezpečné vlastnosti; odpady, jejichž vzniku nelze zabránit, musí být využity, případně odstraněny způsobem, který neohrožuje lidské zdraví a životní prostředí a který je v souladu se zákonem č.185/2001 Sb., o odpadech a se zvláštními právními předpisy a je v souladu s tímto manuálem.
Dodavatel je povinen omezovat a předcházet znečišťování ovzduší a snižovat množství jím vypouštěných znečišťujících látek stanovených podle zákona č.201/2012 Sb., o ochraně ovzduší a prováděcích právních předpisů.
Dodavatel po povinen plnit podmínky stanovené zákonem č.254/2001 Sb., vodní zákon pokud se na něj vztahují.
Dodavatel je povinen dodržovat specifické podmínky stanovené stavebním povolením a projektovou dokumentací a to v oblasti hluku a vibrací.

Povinnosti v oblasti nakládání s odpady

Každý dodavatel před započetím svých činností na stavbě nahlásí, jaké odpady a v jakém množství bude produkovat během své činnosti a zda bude částečně či zcela využívat systému odstraňování odpadů stanoveným zadavatelem nebo sám na svoje náklady. Pokud v hlášení uvede dodavatel nebezpečné odpady, budou součástí hlášení kopie úředních souhlasů k nakládání s nebezpečným odpadem.
V případě, že si bude dodavatel likvidovat část nebo všechny odpady vlastním způsobem a na vlastní náklady, dodá v nejbližší možné době záznam o likvidaci, který bude obsahovat údaje o dodavateli, oprávněnou společnost, které byl odpad předán, množství, druh odpadu a katalogové číslo dle katalogu odpadů. Tato povinnost se vztahuje i na dodavatele produkující odpad, který není součástí systému sběru separovaného odpadu stanoveným zadavatelem.
V případě, že bude dodavatel produkovat nebezpečné odpady, zajistí sám na svoje náklady sběrné nádoby, které budou označeny katalogovým číslem nebezpečného odpadu, názvem odpadu a osobou oprávněnou jednat za dodavatele a jeho telefonního kontaktu. V případě, že nebude možné z kapacitních důvodů použít sběrné nádoby, bude místo nakládání s nebezpečnými odpady zajištěno tak, aby nemohlo dojít k nežádoucímu znehodnocení, odcizení nebo úniku nebezpečných odpadů. Místa nakládání s nebezpečnými odpady budou vždy vybaveny identifikačními listy nebezpečných odpadů.
Likvidaci nebezpečných odpadů v souladu se zákonem potvrzuje příslušný dodavatel dodáním kopií evidenčních listů přepravy nebezpečných odpadů.

Dodavatel je povinen produkovaný odpad třídit a umísťovat do sběrných nádob k tomu určených zadavatelem a to v případě že si sám nezjišťuje jejich odvoz a likvidaci.

Povinnosti v oblasti ochrany ovzduší

Pokud bude dodavatel používat mobilní zdroje znečišťování (dopravní prostředky) je povinen na vyžádání zadavatele předložit záznamy z měření emisí a STK.
Při používání dieselagregátů bude dodavatel používat toto zařízení v souladu s provozními a technickými podmínkami stanovených v manuálu dieselagregátu. Používání těchto zařízení bude v souladu s povinnostmi stanovených zákonem č. 201/2012 Sb., o ochraně ovzduší a navazující legislativy. Při havárii DA viz povinnosti v oblasti ochrany vody.

Povinnosti v oblasti ochrany vody

Dodavatel nebude v objektu zadavatele používat závadné látky (nafta, motorové oleje) stanovené vodním zákonem v rozsahu: v zařízení s celkovým množstvím v něm obsažených závadných látek do 1000 l včetně nebo v přenosných, k tomu určených, obalech s celkovým množstvím v nich obsažených závadných látek do 2000 l včetně. V případě že, bude použití závadných látek nezbytné ve výše uvedeném množství, dotčený dodavatel vypracuje ve havarijní plán úniku závadných látek.
Pokud bude dodavatel během své činnosti používat nebo skladovat závadné látky, budou tyto činnosti zajištěny, tak aby v případě havárie nedošlo k úniku těchto látek do půdy (použití záchytných van). Dodavatel používající závadné látky bude mít k dispozici sorpční sadu pro sanaci v případě úniků nebo úkapů závadných látek. V případě úniků nebo úkapů závadných látek zajistí dodavatel sanaci a odpad ze sanace zlikviduje jako nebezpečný. V případě havarijního úniku tj. do vody nebo kanalizačního řádu, zajistí sanaci v souladu s Vodním zákonem a informuje zástupce zadavatele o provedení.

Povinnosti v oblasti nakládání s chemickými látkami

Dodavatel bude nakládat s chemickými látkami v souladu se zákonem č. 350/2011 Sb., o chemických látkách a chemických směsích a se zákonem č, 258/200 Sb., o ochraně veřejného zdraví. Používané chemické látky budou vždy v řádně označených obalech, dodavatel bude mít k dispozici bezpečnostní listy a s látkami bude nakládáno, tak jak je uvedeno v těchto listech. Prázdné obaly od chemických látek budou považovány za nebezpečný odpad a bude s tímto odpadem nakládáno, tak jak je popsáno v části povinnosti v oblasti nakládání s odpady.

Další ustanovení

Výše uvedené povinnosti je oprávněn průběžně kontrolovat vedoucí oddělení technických služeb. V případě dodavatele, na kterého se vztahují dokumentační povinnosti z výše uvedených povinností, je dodavatel povinen ve stanovených lhůtách zpracovat a předat vedoucímu oddělení technických služeb příslušnou dokumentaci.
Pokud zadavatel obdrží sankce od státní správy a to za nedodržení stanovených povinností dodavatelem, vyhrazuje si zadavatel přenesení sankce v plném rozsahu na dotčeného dodavatele. V případě, že nebude možné identifikovat dodavatele, který zapříčinil neshodu v oblasti nakládání s odpady, bude sankce rozpočítána mezi dodavatele produkující daný odpad na základě množství odpadu.
Dodavatel, pro kterého budou provádět na základě smlouvy činnosti další dodavatelé, se kterými nemá uzavřen smluvní vztah zadavatel, zajistí plnění povinností dodavateli stanovených tímto manuálem. V případě neshody s tímto manuálem bude za její odstranění a následky odpovědný v plném rozsahu dodavatel, který má uzavřený smluvní závazek se zadavatelem.

Tento manuál vychází z povinností stanovených legislativou životního prostředí České Republiky. Před započetím činností dodavatele budou s tímto manuálem seznámeny všechny osoby pracující pro dodavatele, které budou provádět činnosti v rámci objektu ÚPV. Seznámení bude doloženo prezenční listinou obsahující seznam všech osob dodavatele s jejich podpisy potvrzující seznámení s tímto manuálem.

Dodatky a připomínky:

Dodavatel se svým podpisem se zavazuje ke stanoveným povinnostem tohoto manuálu.

Prezenční listina

Pro zakázku:

Podpisem v této listině stvrzuji, že jsem seznámen s manuálem pro dodavatele.

Jméno a příjmení	Název společnosti	datum	podpis

II.
Ostatní ustanovení

2.1 Všechna ostatní ustanovení smlouvy zůstávají nezměněna.
2.2 Dodatek ke smlouvě nabývá platnosti a účinnosti dnem 1.7.2016.

V Praze dne 22.6.2016

za objednatele

.....

Ing. Luděk Churaček
ředitel ekonomického odboru

Úřad průmyslového vlastnictví
Antonína Čermáka 2a
160 68 Praha 6 - Bubeneč
22

V Praze dne 22.6.2016

za zhotovitele

Jan Jeliněk
jednatel

Komterm
ENERGETICKÉ SLUŽBY
KOMTERM Čechy, s.r.o.
Bělehradská 15, 140 00 Praha 4
IČ: [illegible]; DIČ: CZ699001893 (04)