638/18

Kraj Vysočina

108921

KRAJSKÝ ÚŘAD KRAJE Vysočina

Název dokumentu:	Smlouva o zajištění bezpečnosti informací				
Oprávněn/pověřen k podpisu:	~~MUDr. Jiří Běhounek~~ ING. VLADIMÍR NOVOTNÝ				
Schváleno:	RK	**Datum:**	13.2.2018	**Č.usnesení:**	0232/05/2018/RK
Dokument uložen u:	OddPKŽÚ				
Počet vyhotovení:	2				
Adresát:	Projektová kancelář Kraje Vysočina, příspěvková organizace				
Smluvní částka: 1)	0.00				
Odpovědný odbor: 2)	odbor analýz a podpory řízení				
Podpis zajistit do:					

		Pracoviště/pracovník	**Datum**	**Podpis**
Zpracoval:		OAPŘ/Kotrbová	14.2.2018	
Projednáno s:		OAPŘ/Buřičová	14.2.2018	
Právní kontrola:		OAPŘ/Kotrbová	14.2.2018	
Předkládá:		OAPŘ/Kotrbová	14.2.2018	
Potvrzení příjmu smlouvy do předběžné evidence 3)		OAPŘ/Buřičová	14.2.2018	
Zodpovídá:	**~~Příkazce operace:~~**	OAPŘ/Buřičová	14.2.2018	
	~~Správce rozpočtu:~~			

Poznámka:
Subjekt (IČO: 71294376), se kterým je uzavírána smlouva NEBYL NALEZEN v databázi nespolehlivých plátců MFČR; (ověření provedl: kotrbova, datum ověření: 14.02.2018 09:15:02):

Smlouva o zajištění bezpečnosti informací

Rozpočtová skladba:

1) Použije se, pokud se jedná o písemnost typu smlouvy, jejímž předmětem je peněžité plnění. Pokud je v košilce více smluv, uvede se částka souhrnná. Pokud se jedná o smlouvu, příp. smlouvy, u niž je peněžité plnění stanoveno částkou za čerpanou jednotku (např. hodinovou sazbu), uvede se částka maximálního rozsahu tohoto plnění. V případě smluv na dobu neurčitou uveďte částku jedné platby.

2) Odpovědným odborem se rozumí odbor, příp. sekce nebo samostatné oddělení, které za písemnost, její vyřízení a správu záležitosti (správu smluvního vztahu) odpovídá.

3) Potvrzuje vždy vedoucí odpovědného odboru (nenahrazuje právní kontrolu).

Kraj Vysočina

KUJIP016LU8Y

638/18

SMLOUVA O ZAJIŠTĚNÍ BEZPEČNOSTI INFORMACÍ

mezi

1. **Kraj Vysočina**
   se sídlem: Žižkova 57, 587 33 Jihlava
   zastoupený: Ing. Vladimírem Novotným, náměstkem hejtmana
   IČO: 70890749

a

2. **Projektová kancelář Kraje Vysočina, příspěvková organizace**
   se sídlem: Žižkova 1872/89, 58601 Jihlava
   zastoupení: Ing. Erikou Šteflovou, ředitelkou
   IČO: 71294376

   (dále jen „PK KV")

Čl. I
Účel smlouvy

Účelem této smlouvy je zabezpečení informací a informačních aktiv zpřístupněných Krajem Vysočina PK KV při administraci projektů, jejichž nositelem je Kraj Vysočina a administrátorem PK KV. Informace a informační aktivum jsou definovány ve Směrnici, kterou se stanoví bezpečnostní politika Kraje Vysočina, uvedená v příloze č. 2 této smlouvy, v aktuálním znění (dale jen "Směrnice").

Čl. II.
Součinnost smluvních stran

1) PK KV se zavazuje, že pracovníci PK KV budou při administraci projektů dodržovat příslušné vnitřní normy a směrnice Kraje Vysočina, zejména však Směrnici o oběhu a přezkušování účetních dokladů a dále vnitřní předpisy, s nimiž Kraj Vysočina PK KV seznámí či v průběhu trvání této smlouvy bude seznamovat. O seznámení s vnitřními předpisy a předání jejich písemného vyhotovení PK KV bude vždy mezi smluvními stranami sepsán protokol. K seznámení s vnitřními předpisy a k podpisu protokolu o seznámení je za Kraj Vysočina oprávněna Ing. Dana Buřičová, vedoucí Odboru analýz a podpory řízení Krajského úřadu Kraje Vysočina.
2) PK KV se zavazuje vytvářet ze své strany podmínky směřující k minimalizaci případných škod na technickém vybavení Kraje Vysočina.
3) PK KV odpovídá za škody na technickém vybavení Kraje Vysočina, které prokazatelně způsobili pracovníci PK KV.

Čl. III.
Odpovědnost za škodu

1) Každá ze smluvních stran nese odpovědnost za škodu v rámci platných a účinných právních předpisů a této Smlouvy. Obě smluvní strany se zavazují vyvinout maximální úsilí k předcházení škod a k minimalizaci vzniklých škod.
2) Žádná ze smluvních stran neodpovídá za škodu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé smluvní strany. Žádná ze smluvních stran není odpovědná za škodu vzniklou v důsledku prodlení druhé smluvní strany nebo v důsledku nastalých okolností vylučujících odpovědnost dle občanského zákoníku.
3) Smluvní strany se zavazují upozornit druhou smluvní stranu bez zbytečného odkladu na vzniklé okolnosti vylučující odpovědnost bránící řádnému plnění této Smlouvy. Smluvní strany se zavazují vyvinout maximální úsilí k odvrácení a překonání okolností vylučujících odpovědnost.

Čl. IV.
Trvání smlouvy

1) Tato smlouva se uzavírá na dobu neurčitou.
2) Platnost smlouvy lze ukončit písemnou dohodou podepsanou oprávněnými zástupci obou smluvních stran
3) Kterákoliv ze smluvních stran je oprávněna smlouvu vypovědět, a to i bez udání důvodu. Výpovědní lhůta činí 30 kalendářních dnů a začíná běžet první den následující po dni, kdy bylo písemné vyhotovení výpovědi prokazatelně doručeno druhé smluvní straně.

Čl. V.
Bezpečnost informací

1) PK KV je povinna dodržovat platnou legislativu ČR i EU, která se týká bezpečnosti informací.
2) PK KV se zavazuje dodržovat požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv Kraje Vysočina uvedené v příloze č. 1 této smlouvy a Směrnici.
3) PK KV je povinna zajistit plnění bezpečnostních opatření a požadavků stanovených touto smlouvou ve stejné míře u všech případných subdodavatelů či jiných osob, které mají přístup k informačním aktivům Kraje Vysočina prostřednictvím PK KV.
4) PK KV je povinna zachovávat mlčenlivost o všech skutečnostech a informacích, které jí byly v souvislosti s touto smlouvou nebo jejím plněním jakkoliv zpřístupněny, předány či sděleny, nebo o nichž se jakkoliv dozvěděla, vyjma těch, které jsou v okamžiku, kdy se s nimi PK KV seznámila, prokazatelně veřejně přístupné nebo těch, které se bez zavinění PK KV veřejně přístupnými stanou (dále jen „důvěrné informace"). PK KV nesmí důvěrné informace použít v rozporu s jejich účelem, nesmí je použít ve prospěch svůj nebo třetích osob a nesmí je použít ani v neprospěch Kraje Vysočina. Povinnosti dle tohoto odstavce je PK KV povinna zachovávat i po zániku této smlouvy, vyjma případů, kdy se důvěrné informace stanou prokazatelně veřejně přístupné bez zavinění PK KV. Povinnosti dle tohoto odstavce se nevztahují na případy, kdy je PK KV povinna zveřejnit důvěrnou informaci na základě povinnosti uložené PK KV právním předpisem nebo rozhodnutím orgánu veřejné moci.
5) Za nesplnění kterékoliv povinnosti obsažené v této smlouvě, je Kraj Vysočina oprávněn účtovat PK KV smluvní pokutu ve výši 100 000 Kč, a to za každé jednotlivé porušení povinností obsažených v této smlouvě.

Čl. XVI.
Závěrečná ustanovení

1) Tato smlouva může být měněna jen formou písemných, vzestupně číslovaných dodatků podepsaných oprávněnými zástupci obou smluvních stran.
2) Vztahy smluvních stran výslovně touto smlouvou neupravené se řídí obecně závaznými právními předpisy, zejména ustanoveními občanského zákoníku.
3) Nedílnou součástí této Smlouvy jsou Příloha č. 1.
4) Tato smlouva byla sepsána ve dvou vyhotoveních, z nichž každé má povahu originálu. Pro každou smluvní stranu je určeno jedno vyhotovení této smlouvy.

5) Tato smlouva nabývá platnosti dnem podpisu oprávněnými zástupci obou smluvních stran a účinnosti dnem zveřejnění v Registru smluv. Obě smluvní strany souhlasí se zveřejněním celého textu smlouvy včetně podpisů v Registru smluv. Zveřejnění smlouvy v Registru smluv zajistí Kraj Vysočina.

6) Smluvní strany prohlašují, že si smlouvu přečetly, že tato byla sepsána na základě jejich pravé a svobodné vůle, nikoli v tísni a za nápadně nevýhodných podmínek, a na důkaz toho připojují své podpisy.

7) Tato smlouva byla projednána na jednání Rady Kraje Vysočina dne 13. 2. 2018 a o jejím uzavření bylo rozhodnuto usnesením č. 0232/05/2018/RK.

Za PK KV:

V JIHLAVĚ dne 19. 2. 2018

.....
podpis, razítko

Projektová kancelář Kraje Vysočina,
příspěvková organizace
IČ: 712 94 376
Žižkova 1872/89, 586 01 Jihlava

Za Kraj Vysočina:

V Jihlavě dne 15. 2. 2018

.....
podpis, razítko

Kraj Vysočina
Žižkova 57, 587 33 Jihlava

38

Příloha č. 1
Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv Kraje Vysočina

- Bezpečnost přístupových oprávnění
  - PK KV je povinna chránit veškeré přístupové údaje k informačním aktivům Kraje Vysočina včetně přístupů k informačním aktivům PK KV, které umožňují přístup k informačním aktivům Kraje Vysočina či umožnují jejich správu.
  - PK KV je povinna dodržovat tuto bezpečnostní politiku hesel pro výše uvedené přístupové údaje:
    - min. délka hesla 10 znaků
    - složitost hesla musí splňovat minimálně 3 ze 4 kategorií
      - malá písmena
      - velká písmena
      - číslice
      - speciální znaky
    - hesla musí být uchovávána v tajnosti, nesmí být ukládána v nezašifrované podobě (dle bodu kryptografie)
    - hesla nesmí obsahovat žádné informace z přihlašovacího jména (login)
    - platnost hesla musí být maximálně 1 rok.
  - PK KV je povinna používat personifikované účty, které jsou nepřenosné na jiné osoby, než kterým byly údaje přiděleny.
  - Přístupová oprávnění lze využívat pouze pro ten účel, pro který byla zřízena.
  - Pokud by PK KV zřizovala přístupová oprávnění třetí straně, je PK KV povinna o této skutečnosti informovat Kraj Vysočina. Kraj Vysočina má v tomto případě právo zřízení přístupu zamítnout.
- Řízení kybernetických bezpečnostních incidentů:
  - PK KV je povinna na KrÚ hlásit veškeré kybernetické bezpečnostní incidenty, které se týkají informačních aktiv Kraje Vysočina nebo informačních aktiv Poskytovatele, pokud se kybernetický bezpečnostní incident týká informací či informačních aktiv Kraje Vysočina.
  - PK KV je dále povinna poskytnout adekvátní součinnost při řešení kybernetických bezpečnostních incidentů a při forenzní analýze incidentů souvisejících s informačními aktivy Kraje Vysočina.
- Bezpečnost kryptografických prostředků:
  - Pokud PK KV používá kryptografické prostředky v souvislosti s informačními aktivy Kraje Vysočina, je nezbytné, aby použité kryptografické algoritmy byly minimálně v souladu s aktuálním zněním vyhlášky č. 316/2014 Sb.

Kraj Vysočina
KRAJSKÝ ÚŘAD KRAJE VYSOČINA

Směrnice
o řízení rizik informační bezpečnosti Krajského úřadu Kraje Vysočina

ze dne 16. 10. 2017

č. 10/17

Čl. 1
Předmět úpravy

Předmětem této směrnice je stanovení práv a povinností zaměstnanců Kraje Vysočina zařazených do Krajského úřadu Kraje Vysočina (dále jen „zaměstnanci") při řízení rizik, které je prováděno za účelem identifikace zranitelných míst ICT infrastruktury Kraje Vysočina (dále jen „organizace").

Čl. 2
Vymezení pojmů

Pro účely této směrnice se rozumí:

a) **MKB** - manažer kybernetické bezpečnosti.
b) **Garantem aktiva, technickým správcem** - role pro organizaci informační bezpečnosti vymezené směrnicí, kterou se stanoví bezpečnostní politika Kraje Vysočina.
c) **Informačním aktivem, aktivem** - hardware, software, podpůrné systémy, data uložená na počítačích a serverech, data, která jsou posílána přes síť, tištěna nebo napsána na papír, poslána faxem, skenována, uložena na přenosných médiích (CD, DVD, USB disk, diskové pole), vyřčená v rozhovoru, případně sdělena pomocí telefonního přístroje.
d) **Primárním informačním aktivem** – informační systém nebo služba poskytovaná prostřednictvím informačního systému.
e) **Hrozbou** - potencionální příčina bezpečnostní události nebo bezpečnostního incidentu, jejímž výsledkem může být poškození informačního aktiva.
f) **Rizikem** - událost, která může negativně ovlivnit schopnost Krajského úřadu Kraje Vysočina (dále jen „KrÚ") dosáhnout stanovených cílů.
g) **Řízením rizik** - soubor postupů, které vedou k odstranění, zmírnění nebo předcházení rizikům.
h) **DDI** - klíčové parametry pro ohodnocení aktiva, tj. dostupnost, důvěrnost, integrita.

Čl. 3
Identifikace a evidence aktiv

(1) Zaměstnanec, který je v rámci výkonu své činnosti pověřen pořízením nového primárního informačního aktiva, je povinen oznámit MKB, že dojde k pořízení nového informačního aktiva. Proces pořízení informačního aktiva, rozdělení do tříd a klasifikace se řídí směrnicí, kterou se stanoví bezpečnostní politika Kraje Vysočina.

(2) MKB zařadí informační aktivum nejpozději do jeho předání do ostrého provozu do evidence aktiv.

(3) MKB a vedoucí Odboru informatiky Krajského úřad Kraje Vysočina (dále jen „OI") spolu s jednotlivými vedoucími odborů a samostatných oddělení určí konkrétního garanta aktiva.

(4) Vedoucí OI k evidenci aktiv doplní konkrétního technického správce.

(5) MKB spolu s garanty aktiv a technickými správci provádí minimálně 1x ročně nebo v případě zásadní změny aktiva (viz dále) revizi aktiv.

(6) Garant aktiva odpovídá za aktuálnost informací o aktivu (dle principu - každý odpovídá za „své" aktivum, MBK za celý proces) v aplikaci Přehled aktiv. Povinné položky evidence aktiv:
a) název,
b) garant aktiva,
c) technický správce aktiva,
d) hodnota aktiva,
e) stručný popis účelu aktiva,
f) klasifikace.

Čl. 4
Ohodnocení aktiv

(1) Ohodnocení aktiv provádí garanti aktiv ve spolupráci s MKB pravidelně jedenkrát za 12 měsíců pro všechna identifikovaná aktiva organizace. Hodnocení aktiv se provádí formou řízeného interview na výzvu MKB, a to metodou stanovenou v Metodice řízení rizik informační bezpečnosti (dále jen „Metodika").

(2) Ohodnocení aktiv provádí garanti aktiv ve spolupráci s MKB taktéž ad hoc v případě, že dojde k zásadní změně aktiva. Za zásadní změnu aktiva je v tomto případě považováno:
a) významná změna architektury HW,
b) významná změna architektury SW,
c) významná změna organizační struktury,
d) změna lokality používání aktiva,
e) změny v legislativě.

(3) Klasifikace aktiv je vedena v interní aplikaci na Intranetu Krajského úřadu Kraje Vysočina. Za proces ohodnocení aktiv odpovídá MKB, za správné vyjádření hodnoty aktiv odpovídají garanti aktiv a techničtí správci aktiv.

(4) Výsledné hodnoty ohodnocení aktiv křížově ověřují vedoucí odborů a samostatných oddělení, a to jedenkrát za 3 roky formou interview, které iniciuje MKB. V případě, že je rozdíl mezi hodnocením garantem aktiva a vedoucím zaměstnancem vyšší než 2, stanoví konečnou hodnotu aktiva Výbor pro řízení kybernetické bezpečnosti (dále jen „VKB").

Čl. 5
Analýza rizik

(1) Analýza rizik (dále jen „AR") je prováděna dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „zákon"), MKB jednou za 12 měsíců, a to formou detailní analýzy rizik.

(2) AR definuje seznam hrozeb působících na ICT infrastrukturu a stanovuje míru rizika příslušné každému zranitelnému aktivu. Cílem AR je snížení rizika na přijatelnou úroveň, respektive akceptaci zbytkových rizik tam, kde je jejich minimalizace neefektivní. AR zahrnuje tyto činnosti:
a) identifikace hrozeb,
b) identifikace zranitelností,
c) identifikace zavedených protiopatření,
d) hodnocení rizik.

(3) Odpovědné osoby podílející se na analýze rizik jsou:

a) garanti a techničtí správci informačních aktiv kategorie I a II podle Metodiky,
b) vedoucí zaměstnanci zařazení do OI,
c) MKB a architekt kybernetické bezpečnosti.

(4) Podrobný postup provedení AR je uveden v Metodice.

(5) MKB je povinen vypracovat „Závěrečnou zprávu analýzy rizik informační bezpečnosti Krajského úřadu Kraje Vysočina".

Čl. 6
Zvládání rizik

(1) MKB na základě výsledků AR do 30 dnů od ukončení vypracuje dokument „Plán zvládání rizik". Náležitosti „Plánu zvládání rizik" a postup jeho tvorby jsou uvedeny v Metodice.

(2) MKB předloží „Závěrečnou zprávu Analýzy rizik" a „Plán zvládání rizik" VKB k projednání. VKB má právo vrátit dokumenty k dopracování.

(3) VKB na základě dokumentů dle odst. 2 v případě, že hrozící rizika jsou malá, vedou k malým ztrátám a pravděpodobnost jejich výskytu je nízká, nebo v případě jiného důvodu podle svého uvážení vypracuje dokument „Akceptace rizik", který musí obsahovat minimálně tyto položky:
a) název rizika,
b) důvod akceptace,
c) popis, kterého aktiva se riziko týká,
d) seznam protiopatření, včetně vyčíslení cenové i personální náročnosti implementace protiopatření.

(4) VKB předloží „Analýzu rizik", „Plán zvládání rizik" a „Akceptaci rizik" řediteli Krajského úřadu Kraje Vysočina (dále jen „ředitel") ke schválení. Ředitel na základě takto připravené analýzy rozhodne o přijetí navržených opatření resp. akceptaci nebo pověří dotčené odbory realizací opatření. V případě, že opatření spadají do pravomoci orgánů kraje, postoupí ředitel záležitost k rozhodnutí příslušného orgánu kraje.

(5) V případě, že má ředitel výhrady k obsahu provedené analýzy, vrátí dokumenty s uvedením důvodu a návrhu na změnu VKB k přepracování.

Čl. 7
Vyhodnocování řízení rizik

Za vyhodnocování řízení rizik je zodpovědný MKB. Vyhodnocením se rozumí:
a) existující seznam aktiv a jejich vlastníků,
b) existující seznam ohodnocených aktiv z pohledu DDI,
c) definovaný katalog hrozeb,
d) definovaný katalog zranitelností,
e) vypracovaná zpráva hodnotící rizika,
f) definovaný plán zvládání rizik, obsahující termín plnění a odpovědnost.

Čl. 8
Závěrečná ustanovení

(1) Metodika řízení rizik informační bezpečnosti, která provádí a konkretizuje ustanovení této směrnice je umístěna na Procesním portálu krajského úřadu.

(2) Za aktualizaci této směrnice odpovídá Odbor analýz a podpory řízení Krajského úřadu Kraje Vysočina.

(3) Tato směrnice nabývá platnosti dnem podpisu a účinnosti dnem 1. 11. 2017.

V Jihlavě dne 16. 10. 2017

Mgr. Ing. Zdeněk Kadlec, dr. h. c.
ředitel krajského úřadu