Kraj Vysočina

Rada Kraje Vysočina

# Pravidla
# Rady Kraje Vysočina,
# kterými se stanoví
# bezpečnostní politika Kraje Vysočina v oblasti systému řízení bezpečnosti informací

**ze dne 14. 7. 2015**

**č. 06/15**

## Čl. 1
## Úvodní ustanovení

(1) Tato Pravidla Rady Kraje Vysočina**,** kterými se stanoví bezpečnostní politika Kraje Vysočina v oblasti systému řízení bezpečnosti informací (dále jen „Pravidla“), jsou základním strategickým dokumentem zajišťujícím rámec informační bezpečnosti Kraje Vysočina (dále jen „kraj“ nebo „organizace“).

(2) Pravidla se vztahují na veškeré informační systémy a veškeré informace, které jsou v rámci kraje zpracovávány (dále jen „informační aktiva“). Nezáleží přitom na formě uložení informací (počítačové disky, přenosná média, papír, …). Cílem těchto Pravidel je zejména:
a) určit cíle bezpečnostní politiky kraje,
b) určit hlavní zásady bezpečnostní politiky kraje,
c) určit bezpečnostní potřeby bezpečnostní politiky kraje,
d) určit dokumentaci bezpečnostní politiky kraje,
e) určit systém řízení bezpečnosti informací, tj. práva a povinnosti ve vztahu k řízení bezpečnosti informací,
f)zmocnit ředitele Krajského úřadu Kraje Vysočina:
- ke stanovení bezpečnostní politiky v dalších oblastech dle § 5 vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) a
- k zavádění bezpečnostních opatření na základě bezpečnostních potřeb a výsledků hodnocení rizik.

(3) Vedení kraje se tímto dokumentem hlásí k naplňování a dodržování všech zásad informační bezpečnosti, které jsou definovány v tomto a ostatních dokumentech bezpečnostní politiky.

## Čl. 2
## Cíle bezpečnostní politiky kraje

(1) Zajištění požadované úrovně ochrany dostupnosti, důvěrnosti a integrity informačních aktiv organizace.

(2) Veškeré významné uživatelské operace nad informačními aktivy jsou jednoznačně identifikovány, bezpečně zaznamenávány a následně vyhodnocovány

(3) Schopnost detekovat kybernetické bezpečnostní incidenty, a to včetně identifikace původce bezpečnostního incidentu, způsobu narušení bezpečnosti, dopadů a přijetí příslušných reaktivních bezpečnostních opatření.

(4) Zavedení a řízení bezpečnostních opatření a udržování aktualizované bezpečnostní dokumentace a politiky.

(5) Aplikovat systém řízení informační bezpečnosti v organizaci.

## Čl. 3
## Hlavní zásady bezpečnostní politiky kraje

(1) Informační bezpečnost je v organizaci chápána jako komplexní proces ochrany informačních aktiv tvořený opatřeními bezpečnosti lidských zdrojů, fyzické bezpečnosti,

bezpečnosti informačních technologií, plánováním kontinuity činností a zajištěním souladu s požadavky legislativy.

(2) Jsou jasně stanovena pravidla, kompetence a odpovědnosti v oblasti informační bezpečnosti a každý uživatel je s nimi seznámen.

## Čl. 4
## Bezpečnostní potřeby bezpečnostní politiky kraje

Bezpečnostní potřeby pro jednotlivá informační aktiva vychází z jejich kategorizace na základě předchozího ohodnocení a dále z klasifikace zpracovávaných informací.

## Čl. 5
## Bezpečnostní politika kraje

(1) Celkový systém bezpečnostní politiky v organizaci je vypracován v souladu:
a) s mezinárodní normou Information Security Management System (Systém řízení bezpečnosti informací) – ISO IEC 27001:2013 (dále jen „ISMS“),
b) se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a souvisejících právních předpisech,
c) se zákonem č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů,
d) s ostatními požadavky danými obecně závaznými právními předpisy,
e) s úrovní rizik, která hrozí informačním aktivům organizace,
f)s potřebami organizace v oblasti zpracování a ochrany informací.

(2) Bezpečnostní politiku tvoří dokumenty tří úrovní:
a) tato Pravidla - začleňují bezpečnost informací do kontextu celkové bezpečnosti organizace a definují základní bezpečnostní principy,
b) směrnice - definují požadovanou úroveň bezpečnosti v konkrétních oblastech činnosti organizace. Primárním cílem je identifikace všech oblastí organizace relevantních pro implementaci ISMS a definice úrovně ochrany informačních zdrojů používaných organizací proti relevantním typům ohrožení,
c) příkazy ředitele - obsahují zpravidla popis realizace vybraných bezpečnostních prvků a bezpečnostních opatření pro konkrétní principy politiky a konkrétní bezpečnostní potřeby. Obsahují technické údaje popisující použitý software, hardware, použitá procedurální či organizační opatření a způsob jejich implementace. Definují pracovní postupy nezbytné pro dodržení bezpečnostních potřeb.

## Čl. 6
## Systém řízení bezpečnosti informací

(1) Systém řízení bezpečnosti informací je založen na mezinárodní normě ISMS a v souladu s vyhláškou o kybernetické bezpečnosti.

(2) K zajištění informační bezpečnosti v organizaci jsou definovány následující role:
a) manažer kybernetické bezpečnosti,
b) architekt kybernetické bezpečnosti,
c) auditor kybernetické bezpečnosti,
d) garant aktiva,
e) technický správce aktiva,
f)výbor pro řízení informační bezpečnosti,
Výkon role auditora kybernetické bezpečnosti je oddělen od výkonu rolí dle Čl. 6 odst. 2 písm. a), b), d) a e) těchto Pravidel.

(3) V organizaci jsou prováděna nezávislá přezkoumání formou auditu:
a) celkového systému řízení informační bezpečnosti (ISMS),
b) aktuálnosti a správnosti bezpečnostní dokumentace,
c) aktuálního stavu bezpečnostních opatření,
d) dle aktuální potřeby.

(4) V organizaci jsou řízena aktuální rizika informačních aktiv a k nim stanoveny relevantní hrozby, zranitelnosti a možné dopady.

**Čl. 7**
**Oblasti relevantní pro implementaci ISMS – předmět ochrany**

(1) Pro kraj jsou definované hranice ISMS vymezeny pro oblasti uvedené v § 5 odst. 1 vyhlášky o kybernetické bezpečnosti č. 316/2014 Sb., tj:
a) systém řízení bezpečnosti informací,
b) organizační bezpečnost,
c) řízení vztahů s dodavateli,
d) klasifikace aktiv,
e) bezpečnost lidských zdrojů,
f) řízení provozu a komunikací,
g) řízení přístupu,
h) bezpečné chování uživatelů,
i) zálohování a obnova,
j) bezpečné předávání a výměna informací,
k) řízení technických zranitelností,
l) bezpečné používání mobilních zařízení,
m) poskytování a nabývání licencí programového vybavení a informací,
n) dlouhodobé ukládání a archivace informací,
o) ochrana osobních údajů,
p) fyzická bezpečnost,
q) bezpečnost komunikační sítě,
r) ochrana před škodlivým kódem,
s) nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí,
t) využití a údržba nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí a
u) používání kryptografické ochrany.

(2) Bezpečnostní politiku v těchto dalších oblastech stanoví na základě bezpečnostních potřeb a výsledků hodnocení rizik ředitel Krajského úřadu Kraje Vysočina, a to včetně zavedení příslušných bezpečnostních opatření.

**Čl. 8**
**Závěrečná ustanovení**

(1) Za aktualizaci Pravidel odpovídá manažer kybernetické bezpečnosti (Čl. 6 odst. 2a).

(2) Pravidla nabývají platnosti a účinnosti dnem schválení Radou Kraje Vysočina.

(3) Pravidla byla projednána na jednání Rady Kraje Vysočina dne 14. 7. 2015 a schválena usnesením 1296/22/2015/RK.

V Jihlavě dne 14. 7. 2015

MUDr. Jiří Běhounek
hejtman kraje