Kraj Vysočina

Rada Kraje Vysočina

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

**ze dne 3. 12. 2019**

**č. 09/19**

## 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“), a to bez ohledu na formu jejich uložení. Cílem těchto Pravidel je zejména:
a) vymezit cíle bezpečnostní politiky kraje,
b) definovat hlavní zásady bezpečnostní politiky kraje,
c) určit bezpečnostní potřeby bezpečnostní politiky kraje,
d) vymezit systém řízení bezpečnosti informací, tj. práva a povinnosti ve vztahu k řízení bezpečnosti informací a oblasti relevantní pro implementaci ISMS – předmět ochrany.

(3) Kraj Vysočina se tímto dokumentem hlásí k naplňování a dodržování všech zásad informační bezpečnosti, které jsou definovány v těchto Pravidlech a ostatních dokumentech bezpečnostní politiky.

## Čl. 2
## Cíle bezpečnostní politiky kraje

Cíly bezpečnostní politiky kraje jsou:
a) zajištění požadované úrovně ochrany dostupnosti, důvěrnosti a integrity informačních aktiv kraje,
b) schopnost detekovat kybernetické bezpečnostní incidenty, a to včetně identifikace původce bezpečnostního incidentu, způsobu narušení bezpečnosti, dopadů a přijetí příslušných reaktivních bezpečnostních opatření,
c) zavedení a řízení bezpečnostních opatření a udržování aktualizované bezpečnostní dokumentace a politiky,
d) plánování, provozování, kontrola a zlepšování zavedeného systému řízení bezpečnosti informací.

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

Hlavní zásady bezpečnostní politiky kraje jsou:
a) 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,
b) 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, z analýzy rizik a aktuálních bezpečnostních trendů.

## Čl. 5
## Politika bezpečnosti informací kraje

(1) Celkový systém politiky bezpečnosti informací 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, ve znění pozdějších předpisů (dále jen „ZKB“),
c) se zákonem č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů,
d) s ostatními požadavky danými obecně závaznými právními předpisy,
e) s úrovní rizik, která hrozí informačním aktivům organizace,
f) s potřebami organizace a aktuálními bezpečnostními trendy 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) Strategie kvality Kraje Vysočina – blíže určují koncepci ISMS,
c) vnitřní řízená dokumentace - definuje požadovanou úroveň bezpečnosti v konkrétních oblastech činnosti organizace.

Primárním cílem bezpečnostní politiky je identifikace všech oblastí relevantních pro implementaci ISMS a definice úrovně ochrany informačních zdrojů používaných organizací proti relevantním typům ohrožení. Popisuje realizaci vybraných bezpečnostních prvků a bezpečnostních opatření pro konkrétní principy politiky a konkrétní bezpečnostní potřeby. Obsahuje technické údaje popisující použitý software, hardware, použitá procedurální či organizační opatření a způsob jejich implementace. Definuje 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 na souladu se ZKB.

(2) K zajištění informační bezpečnosti v organizaci jsou definovány následující role:
a) manažer a architekt kybernetické bezpečnosti,
b) auditor kybernetické bezpečnosti,
c) garant aktiva,
d) technický správce aktiva,
e) 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 a
c) aktuálního stavu bezpečnostních opatření.

(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 tyto oblasti, které jsou v souladu se ZKB a ISMS:
a) systém řízení bezpečnosti informací,
b) řízení rizik,
c) bezpečnostní politika,
d) organizační bezpečnost,
e) stanovení bezpečnostních požadavků pro dodavatele,
f) řízení aktiv,
g) bezpečnost lidských zdrojů,
h) řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému,
i) řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému,
j) akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů,
k) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
l) řízení kontinuity činností
m) kontrola a audit informačních systémů,
n) fyzická bezpečnost,
o) nástroj pro ochranu integrity komunikačních sítí,
p) nástroj pro ověřování identity uživatelů,
q) nástroj pro řízení přístupových oprávnění,
r) nástroj pro ochranu před škodlivým kódem,
s) nástroj pro zaznamenávání informačních systémů, jejich uživatelů a administrátorů,
t) nástroj pro detekci kybernetických bezpečnostních událostí,
u) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,
v) aplikační bezpečnost,
w) kryptografické prostředky,
x) nástroje pro zajišťování úrovně dostupnosti informací.

(2) Bezpečnostní politiku v oblastech dle odst. 1 a případně dalších pravidly neupravených oblastech dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů, a dle dalších souvisejících právních předpisů stanoví na základě bezpečnostních potřeb a výsledků hodnocení rizik ředitel Krajského úřadu Kraje Vysočina, a to včetně zavedení příslušných bezpečnostních opatření.

(3) Ředitel Krajského úřadu Kraje Vysočina je dále zmocněn k zavádění bezpečnostních opatření na základě aktuálních bezpečnostních potřeb a výsledků hodnocení rizik a k určení rozsahu systému řízení bezpečnosti informací v rámci vydávaných vnitřních předpisů organizace.

## Čl. 8
## Závěrečná ustanovení

(1) Za aktualizaci Pravidel odpovídá Odbor analýz a podpory řízení Krajského úřadu Kraje Vysočina.

(2) Tato Pravidla ruší 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.

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

(4) Pravidla byla projednána na jednání Rady Kraje Vysočina dne 3. 12. 2019 a schválena usnesením 2035/36/2019/RK.

V Jihlavě dne 3. 12. 2019

MUDr. Jiří Běhounek
hejtman kraje