SMĚRNICE

RADY OLOMOUCKÉHO KRAJE

ze dne 24. 7. 2023 č. 1/2023

kterou se vydává

Bezpečnostní politika informací

Rada Olomouckého kraje vydává svým usnesením č. …../ …… ze dne 24. 7. 2023 tuto směrnici:

OBSAH

Čl. 1
Úvodní ustanovení

(1) Účel

a) Účelem dokumentu Bezpečnostní politika informací je stanovit cíle, princip, potřeby, rozsah a hranice Systému řízení bezpečnosti informací (dále jen „SŘBI“) u Olomouckého kraje a současně stanovit pravidla pro bezpečný provoz a správu informačních systémů provozovaných v SŘBI.

b) Pravidla stanovená tímto dokumentem obsahují postupy, které vycházejí z požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), navazující vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) a bezpečnosti informací, zejména dle ČSN EN ISO/IEC 27001.

(2) Závaznost

Bezpečnostní politika informací je závazná pro všechny zaměstnance Olomouckého kraje a uvolněné členy Rady Olomouckého kraje. V případě přístupu extérních subjektů k aktivům Olomouckého kraje je externí subjekt seznámen s relevantními pravidly této politiky, k jejichž dodržování je zavázán zapracováním vybraných pravidel do smlouvy.

Čl. 2
Vymezení pojmů

(1) Použité zkratky

AD	Adresářová služba (Active Directory)
BCM	Řízení kontinuity činností (Business Continuity Management)
BIA	Analýza dopadů (Business Impact Analysis)
CCTV	Uzavřený televizní okruh (Closed Circuit Television)
EPS	Elektrická požární signalizace
ERP	Plánování podnikových zdrojů (Enterprise Resource Planning)
GDPR	Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation)
GovCERT/ CSIRT	Speciální vládní skupina zabývající se poskytováním bezpečnostních rad (Government Computer Emergency Response Team) Skupina pro reakci na počítačové bezpečnostní události (Computer Security Incident Response Team)
HW	Hardware. Označuje veškeré fyzicky existující technické vybavení počítače.
ICT	Informační a komunikační technologie (Information and Communication Technologies). Označuje veškeré technologie používané pro komunikaci a práci s informacemi.
IDM	Jednotný identifikační systém (Identity Management)
IS	Informační systém. Systém pro sběr, udržování, zpracování a poskytování informací a dat.
ISDS	Informační systém datových schránek

IS SŘBI	Informační systém systému řízení bezpečnosti informací
IT	Informační technologie
KB	Kybernetická bezpečnost
KBI	Kybernetický bezpečnostní incident
KBU	Kybernetická bezpečnostní událost
KÚOK	Krajský úřad Olomouckého kraje
LAN	Lokální síť (Local Area Network)
MDM	Správa mobilních zařízení (Mobile Device Management)
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OIT	Odbor informačních technologií
OK	Olomoucký kraj
OS	Operační systém
PIN	Osobní identifikační číslo (Personal Identification Number)
PS KB	Pracovní skupina kybernetické bezpečnosti
PZTS	Poplachové zabezpečovací a tísňové systémy
RPO	Bod obnovy dat (Recovery Point Objective)
RTO	Doba obnovy chodu (Recovery Time Objective)
SLA	Service level agreement = úroveň podpory služby
SSL	Spisové služba
SSL protokol	Zabezpečení komunikace šifrováním a autentizaci komunikujících stran (Secure Sockets Layer)
SŘBI	Systém řízení bezpečnosti informací
SW	Software. Programové vybavení.
TCK	Technologické centrum kraje
UPS	Zdroj nepřerušovaného napájení (Uninterruptible Power Supply/Source)
VIS	Významný informační systém
VoKB	Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
VP	Vnitřní předpis
VPN	Virtuální privátní síť
VŘKB	Výbor pro řízení kybernetické bezpečnosti
WI-FI	Komunikační standard pro bezdrátový přenos dat (Wireless Fidelity)
ZoKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

(2) Definice

a) **Primární aktivum** je informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikačním systém.

b) **Podpůrné aktivum** je technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému. Podpůrná aktiva obdobného typu se mohou seskupovat do takzvaných „typových aktiv".

c) **Technické aktivum** je takové technické vybavení, komunikační prostředky a programová vybavení informačního a komunikačního systému a objekty, ve kterých jsou tyto systémy umístěny, jejichž selhání může mít dopad

na informační a komunikační systém**.**

d) **Typové aktivum** je množina seskupených podpůrných aktiv obdobného typu.
e) **Informační aktivum** jsou informace a data, která jsou zpracovávány OK v listinné i elektronické podobě.
f) **Hrozba** je potenciální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, která může způsobit škodu.
g) **Riziko** vyjadřuje míru ohrožení aktiva, míru nebezpečí, že se uplatní hrozba a dojde k nežádoucímu výsledku vedoucímu ke vzniku škody (dopadu hrozby).
h) **Akceptovatelné riziko** je přijatelné riziko, které není nutné zvládat pomocí dalších bezpečnostních opatření.
i) **Analýza rizik** zahrnuje ohodnocení kombinace hrozby a zranitelnosti s ohledem na aktiva a výpočet finální hodnoty výše rizika.
j) **Bezpečnost informací** je zajištění důvěrnosti, integrity a dostupnosti informací a dat.
k) **Bezpečnostním opatřením** se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru.
l) **Dostupnost** je vlastnost přístupnosti a použitelnosti aktiva na žádost oprávněné entity.
m) **Důvěrnost** je vlastnost, že informace není dostupná nebo není odhalena neoprávněným osobám, entitám nebo procesům.
n) **Garant smlouvy** je zaměstnanec odpovědný za přípravu smlouvy s dodavatelem, který současně odpovídá za přípravu technické specifikace předmětu dodávky nebo služby. Technickou specifikaci obvykle připravuje zaměstnanec, garantující potřebné odborné znalosti. Současně odpovídá za realizaci smlouvy v rozsahu smluvně stanovených parametrů kvality zajišťované dodávky nebo služby a za výkon kontroly dodávky nebo služby.
o) **Integrita** je vlastnost přesnosti a úplnosti aktiv.
p) **Správce významného informačního systému** – Olomoucký kraj, který určuje účel zpracování informací a podmínky provozování významného informačního systému.
q) **Provozovatel významného informačního systému** – Olomoucký kraj, který zajišťuje funkčnost technických a programových prostředků tvořících významný informační systém.
r) **Kybernetická bezpečnost** je zajištění digitálního prostředí tvořeného informačními systémy, službami a sítěmi elektronických komunikací, umožňující bezpečný vznik, zpracování a výměnu informací.
s) **Událost, Incident** je jakékoli narušení běžné činnosti.
t) **Provozní událost** je událost, která vznikla jako následek nestandardní činnosti technického aktiva, u které lze vyloučit jako příčinu úmysl či záměr.
u) **Kybernetická bezpečnostní událost** je událost, která může způsobit narušení bezpečnosti informací v SŘBI a VIS a tím způsobit nedostupnost nebo snížení kvality a omezení poskytování služby informačního a komunikačního systému.
v) **Kybernetický bezpečnostní incident** je narušení bezpečnosti informací v SŘBI a VIS, které způsobí nedostupnost nebo snížení kvality a omezení poskytování služby informačního a komunikačního systému. (Plánované servisní zásahy do VIS nejsou kybernetickým bezpečnostním incidentem za předpokladu, že rozsah zásahu do VIS nepřesáhne plánovaný rámec zásahu. Obdobně nejsou hodnoceny jako kybernetický bezpečnostní incident

plánované odstávky dodávek elektrické energie).

w) **Mimořádná událost** je bezpečnostní incident v hranicích SŘBI, VIS, technická porucha, útok, požár, živelní pohroma nebo jakákoli jiná závažná událost, kterou není možné řešit běžnými provozními postupy a která může způsobit přerušení nebo omezení poskytování základní služby či služeb IS SŘBI.

x) **Zranitelnost** je slabé místo aktiva nebo slabé místo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami.

y) **Uživatel** je zaměstnanec Olomouckého kraje, uvolněný člen Rady Olomouckého kraje a externí subjekt s přístupem k aktivům Olomouckého kraje, který je seznámen s relevantními pravidly této politiky, k jejichž dodržování je zavázán zapracováním vybraných pravidel do smlouvy.

z) **Služební zařízení** je prostředek ICT, který je přidělen uživateli k plnění pracovních povinností zaměstnavatelem, zejména obvykle pracovní stanice, samostatný počítač, tiskárna, kopírka, scanner a další případná HW zařízení vybavená potřebným programovým vybavením.

aa) **Přenosné zařízení** je služební mobilní zařízení ICT. V podmínkách OK se obvykle jedná o notebook, tablet, smartphone, čtečka dat.

bb) **Vyměnitelné médium** je přenosné elektronické paměťové médium (datový nosič), které lze vložit nebo připojit k počítačovému zařízení a vyjmout z něj, či odpojit od něj, zejména magnetické, optické nebo polovodičové zařízení. Slouží k ukládání textových, obrazových a zvukových záznamů a informací. V podmínkách OK se obvykle jedná o pevné disky, USB disk, flash disky, externí disky, paměťové karty, CD, DVD.

cc) **Dodavatel** je dodavatel, který zajišťuje dodávky nebo služby, které jsou poskytovány v hranicích SŘBI, ale nesouvisí s provozem VIS.

dd) **Významný dodavatel** je dodavatel, který zajišťuje, na základě smluvního vztahu s OK, dodávky nebo služby, které jsou poskytovány v hranicích VIS, služba a informace VIS jsou na nich částečně závislé, ale jejich nedostupnost či přerušení nemůže zásadním způsobem ovlivnit bezpečnost, kvalitu a dostupnost poskytované služby a informací VIS.

ee) **Významný dodavatel v roli provozovatele VIS** je dodavatel, který zajišťuje, na základě smluvního vztahu s OK, dodávky nebo služby zajišťující funkčnost technických a programových prostředků VIS, které jsou poskytovány v hranicích VIS, služba a informace VIS jsou na nich závislé a jejich nedostupnost či přerušení může zásadním způsobem ovlivnit bezpečnost, kvalitu a dostupnost poskytované služby a informací VIS.

ff) **Bod obnovy dat – Recovery Point Objective (RPO)** - Bod obnovy dat informačního a komunikačního systému nezbytný pro zajištění poskytování minimální úrovně služby tohoto systému.

gg) **Doba obnovy chodu – Recovery Time Objective (RTO)** - Doba obnovy chodu informačního a komunikačního systému nezbytná pro zajištění poskytování minimální úrovně služby tohoto systému.

hh) **Software** - (programové vybavení) je sada všech počítačových programů v počítači. Software zahrnuje aplikační software (pracuje s ním uživatel), operační systém (zajišťuje běh programů) a další.

Čl. 3
Systém řízení bezpečnosti informací

Čl. 4
Řízení aktiv a rizik

Čl. 5
Organizační bezpečnost a bezpečnostní role

Čl. 6
Řízení dodavatelů

Čl. 7
Bezpečnost lidských zdrojů

Čl. 8
Řízení provozu a komunikací

Čl. 9
Řízení přístupu

Čl. 10
Řízení změn

Čl. 11
Akvizice, vývoj a údržba

Čl. 12
Bezpečnost komunikačních sítí

Čl. 13
Fyzická bezpečnost

Čl. 14
Detekce kybernetických bezpečnostních událostí

Čl. 15

Aplikační bezpečnost

Čl. 16
Kryptografická ochrana

Čl. 17
Zrušovací ustanovení

Touto směrnicí se zrušuje Směrnice Olomouckého kraje ze dne 22. 6. 2020, kterou se vydává Systém řízení bezpečnosti informací.

Čl. 18
Účinnost

Tato směrnice nabývá účinnosti dne 1. 8. 2023.