**SMĚRNICE RADY KRAJE**

**č. 1/2019**

k politice řízení bezpečnosti informací

Účinnost od 15. 05. 2019

 **Obsah**

[I. Úvodní ustanovení 6](#_Toc534875605)

[II. Rozsah a hranice SŘBI 7](#_Toc534875606)

[1. Vnitřní a vnější vlivy na SŘBI 7](#_Toc534875607)

[2. Působnost, Fyzické a Logické hranice SŘBI 7](#_Toc534875608)

[3. Kontakt s příslušnými orgány a autoritami a zájmovými skupinami 8](#_Toc534875609)

[4. Pravidla a postupy pro řízení zdrojů a provozu SŘBI 8](#_Toc534875610)

[5. Bezpečnost informací v řízení projektů 9](#_Toc534875611)

[6. Pravidla a postupy pro provádění auditů 10](#_Toc534875612)

[7. Pravidla a postupy pro nápravná opatření a zlepšování systému řízení bezpečnosti informací 10](#_Toc534875613)

[III. Závěrečná ustanovení 10](#_Toc534875614)

Příloha č. 1 - Politika řízení aktiv

Příloha č. 2 - Politika organizační bezpečnosti

Příloha č. 3 - Politika řízení dodavatelů

Příloha č. 4 - Politika bezpečnosti lidských zdrojů

Příloha č. 5 - Politika řízení provozu a komunikací

Příloha č. 6 - Politika řízení přístupu

Příloha č. 7 - Politika bezpečného chování uživatelů

Příloha č. 8 - Politika zálohování a obnovy a dlouhodobého ukládání

Příloha č. 9 - Politika bezpečného předávání a výměny informací

Příloha č. 10 - Politika řízení technických zranitelností

Příloha č. 11 - Politika bezpečného používání mobilních zařízení

Příloha č. 12 - Politika akvizice, vývoje a údržby

Příloha č. 13 - Politika ochrany osobních údajů

Příloha č. 14 - Politika fyzické bezpečnosti

Příloha č. 15 - Politika bezpečnosti komunikační sítě

Příloha č. 16 - Politika ochrany před škodlivým kódem

Příloha č. 17 - Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí

Příloha č. 18 - Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí

Příloha č. 19 - Politika bezpečného používání kryptografické ochrany

Příloha č. 20 - Politika řízení změn

Příloha č. 21 - Politika zvládání kybernetických bezpečnostních incidentů

Příloha č. 22 - Politika řízení kontinuity činností

SEZNAM POUŽITÝCH ZKRATEK

|  |  |  |
| --- | --- | --- |
| BS |  | Bezpečnostní správce |
| CERT (CSIRT.CZ) |  | Mezinárodních uskupení ICT bezpečnostních týmů CSIRT (Computer Security Incident Response Team) a CERT (Computer Emergency Response Team). |
| ČSN ISO/IEC 27001:2014 |  | Norma z oblasti bezpečnosti informací. |
| DPO |  | Data Protection Officer – Pověřenec pro ochranu osobních údajů, Manažer kvality a Manažer rizik |
| EPS |  | Elektronický požární systém |
| HW |  | Hardware |
| ICT |  | Informační a komunikační technologie |
| IS |  | Informační systém |
| ISVS |  | Informační systém veřejné správy (soubor informačních systémů), které slouží pro výkon veřejné správy – viz § 3 odst. 1 zák. č. 365/2000 Sb.) |
| KS |  | Komunikační systém |
| krajský úřad |   | Krajský úřad Libereckého kraje |
| LK |  | Liberecký kraj |
| MKB |   | Manažer kybernetické bezpečnosti |
| NTB |  | Notebook |
| NTP |  | Network Time Protocol - protokol zajišťuje, aby všechny počítače v síti měly stejný a přesný čas |
| NÚKIB |   | Národní úřad pro kybernetickou a informační bezpečnost |
| OI |  | Odbor informatiky |
| PBI |  | Politika bezpečnosti informací, zpravidla jako součást systému řízení bezpečnosti informací v organizaci, která je platná pro celou organizaci |
| PC |  | Počítač – pevná stanice |
| Protokol FTP |  | File Transfer Protocol - protokol pro přenos souborů mezi počítači pomocí externí počítačové sítě. |
| Protokol SSH |  | Secure Shell - program a zároveň protokol pro zabezpečenou komunikaci v počítačových sítích |
| Protokol HTTPS |  | Šifrovaný protokol HTTP pro přenos webových stránek |
| PZTS |  | Poplachový zabezpečovací a tísňový systém |
| Rada |  | Rada Libereckého kraje |
| SLA |  | Service Level Agreement – Smlouva o stanovení úrovně poskytovaných služeb |
| SMTP, POP3 |  | Protokoly elektronických poštovních služeb |
| SŘBI |   | Systém řízení bezpečnosti informací |
| SW |  | Software |
| 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) |
| VPN |  | Virtual Private Network - prostředek k propojení několika počítačů prostřednictvím (veřejné) nedůvěryhodné počítačové sítě |
| VŘKB |  | Výbor pro řízení kybernetické bezpečnosti |
| Zákon o ISVS |  | Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, v platném znění |
| Zastupitelstvo |  | Zastupitelstvo Libereckého kraje |
| ZoKB |   | Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) |

# I. Úvodní ustanovení

Směrnice Rady Libereckého kraje je navržena pro účely zajištění optimálního systému řízení bezpečnosti informací (dále jen „SŘBI“) Libereckého kraje a Krajského úřadu Libereckého kraje, který současně realizuje požadavky kybernetické bezpečnosti vyplývající ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti, dále jen „ZoKB“).

Bezpečnostní opatření jsou rozdělena do jednotlivých oblastí bezpečnosti. Pro každou oblast bezpečnosti SŘBI je ustanoven její garant, který řídí realizaci opatření a odpovídá za stav bezpečnosti ve své oblasti.

SŘBI je v kontextu zajištění kybernetické bezpečnosti realizován v následujících oblastech bezpečnosti:

* systému řízení bezpečnosti informací,
* řízení aktiv,
* organizační bezpečnosti,
* řízení dodavatelů,
* bezpečnosti lidských zdrojů,
* řízení provozu a komunikací,
* řízení přístupu,
* bezpečného chování uživatelů,
* zálohování a obnovy a dlouhodobého ukládání,
* bezpečného předávání a výměny informací,
* řízení technických zranitelností,
* bezpečného používání mobilních zařízení,
* akvizice, vývoje a údržby,
* ochrany osobních údajů,
* fyzické bezpečnosti,
* bezpečnosti komunikační sítě,
* ochraně před škodlivým kódem,
* nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí,
* využití a údržba nástroje pro sběr vyhodnocení kybernetických bezpečnostních událostí,
* bezpečného používání kryptografické ochrany,
* řízení změn,
* zvládání kybernetických bezpečnostních incidentů,
* řízení kontinuity činností.

Oblasti jsou navrženy tak, aby v rámci každé oblasti bylo možno do určité míry samostatně aplikovat principy bezpečnostní politiky.

Základní principy řízení bezpečnosti informací jsou definovány na základě nejlepší praxe,
v oblasti řízení bezpečnosti a opírají se o požadavky relevantní legislativy České republiky
a normy systému bezpečnosti informací ČSN ISO/IEC 27001:2014. Jedná se o následující základní principy:

* bezpečnost musí být navrhována tak, aby působila vyváženě ve všech oblastech bezpečnosti a chránila všechna důležitá aktiva. Zásady bezpečnosti musí být prosazovány do všech činností realizovaných v rámci LK a krajského úřadu,
* dokumentování informací o SŘBI, což se týká především řídících dokumentací, analýz v rámci SŘBI, plánů a záznamů o jejich plnění, zápisů z jednání, systémové logy, příručky pro obsluhy, metodiky a hlášení kybernetického bezpečnostního incidentu dle ZoKB,
* předpokladem kvalitní ochrany aktiv je jejich identifikace, určení osob nesoucích osobní odpovědnost za jejich ochranu a stanovení, jakým způsobem se s nimi může nakládat,
* bezpečnost informací je nastavena a zajištěna na základě vyhodnocení rizik bezpečnosti informací tak, aby opatření byla přiměřená hrozbám, k tomu jsou nastaveny základní procesy pro posuzování a ošetření rizik,
* udržování povědomí zainteresovaných osob o SŘBI a dodržování stanovených pravidel,
* monitoring a měření účinnosti SŘBI, včetně pravidelných nezávislých auditů
a přezkumů vedením,
* kontrola a přezkoumávání účinnosti bezpečnostních opatření a jejich neustálé zlepšování stejně jako zlepšování celého procesu řízení a používaných nástrojů pro zajištění adekvátnosti ochrany v souvislosti s dalším vývojem ICT, novými hrozbami a souvisejícími riziky,
* oddělení výkonných, kontrolních a auditních povinností tak, aby bylo sníženo riziko pro neoprávněné nebo nekalé praktiky v realizaci SŘBI.

Bezpečnostní cíle systému řízení bezpečnosti informací jsou:

* realizace jednotných postupů, které jsou v souladu se touto směrnicí, přílohami a dalšími navazujícími směrnicemi,
* řízení a klasifikace aktiv,
* řízení provozu informačních a komunikačních systémů a technologií,
* prosazování principů bezpečnosti informací do nákupu a vývoje nových informačních systémů,
* realizace plánování kontinuity informačních a komunikačních systémů a technologií,
* kontrola dodržování stanoveného komplexu opatření a vyhodnocování případů porušování zásad bezpečnosti informačních a komunikačních technologií,
* pravidelné seznamování zaměstnanců se zásadami a požadavky bezpečnosti informačních a komunikačních technologií.

# Rozsah a hranice SŘBI

## Vnitřní a vnější vlivy na SŘBI

Vnitřně je vliv na SŘBI ovlivňován především vnitřní organizační strukturou krajského úřadu. Dalším významným vnitřním prvkem pro dosažení zamýšlených výstupů je Rada a Zastupitelstvo, které svými zákonem danými pravomocemi mohou krajský úřad úkolovat a tím také pozměnit již dříve nastavené předpokládané výstupy systému řízení bezpečnosti informací.

Z vnějšího prostředí působí na SŘBI změny obsahu a rozsahu bezpečnostních opatření stanovovaných především ZoKB, jeho prováděcími vyhláškami a další legislativou ČR a EU. V důsledku těchto změn musí být následně upravován soubor zásad a pravidel (bezpečnostní politiky), které určují způsob zajištění ochrany aktiv.

## Působnost, Fyzické a Logické hranice SŘBI

**Působnost** SŘBI zahrnuje všechny uživatele využívající ICT LK a další osoby či kooperující organizace, které se vyskytují v níže uvedených fyzických lokalitách. Dále zahrnuje také kooperující subjekty sídlící mimo fyzické hranice, které využívají ICT technologie LK s umožněním vzdáleného přístupu do ICT kyberprostoru LK.

**Fyzické hranice** působnosti SŘBI pokrývají všechny objekty a prostory hlavní a záložní lokality, tj.:

***Hlavní lokalita***

|  |  |  |
| --- | --- | --- |
| Krajský úřad Libereckého kraje U Jezu 642/2a 461 80 Liberec 2  | a | Krajský úřad Libereckého kraje Evropský důmU Jezu 525/4 461 80 Liberec 2  |

***Záložní lokalita***

Magistrát města Liberce

Budova Uran

serverovna 1 NP

1. máje 108

460 07 Liberec 2

**Logické hranice působnosti** SŘBI se vztahují na všechny ICT systémy, které jsou ve správě LK (až po hraniční prvky – routery a firewally), případně jejichž správou je legislativně nebo smluvně pověřen externí subjekt, a které nakládají s informačními aktivy LK.

## Kontakt s příslušnými orgány a autoritami a zájmovými skupinami

Kontakt s příslušnými orgány a autoritami a zájmovými skupinami slouží k tomu, aby byly zajištěny hlavní bezpečnostní cíle LK a krajského úřadu a bylo zajištěno, aby aktiva LK a krajského úřadu byla adekvátně chráněna na základě aktuálních hrozeb a zranitelností a aby bylo dosaženo bezpečnostních cílů SŘBI LK.

Manažer kybernetické bezpečnosti sleduje zájmové webové stránky a tím si udržuje povědomí o bezpečnostních hrozbách, které by mohly ohrozit bezpečnost informací na krajském úřadě.

Případné členství dalších zaměstnanců krajského úřadu ve zvláštních zájmových skupinách se využívá zejména k:

* zlepšování znalostí o doporučených postupech a sledování aktuálního vývoje
v příslušné oblasti bezpečnosti informací,
* obdržení včasných varování, doporučení a oprav týkajících se útoků a zranitelností,
* získání přístupu k doporučením specialistů bezpečnosti informací,
* sdílení a výměně informací o nových technologiích, produktech, hrozbách nebo zranitelnostech,
* zajištění vhodných styčných míst při řešení bezpečnostních incidentů.

## Pravidla a postupy pro řízení zdrojů a provozu SŘBI

Vedení LK a vedení krajského úřadu zajistí stanovení bezpečnostní politiky a cílů SŘBI a zavazuje se k plné podpoře SŘBI, zejména k zajištění a poskytnutí nezbytných zdrojů pro zajištění správného chodu SŘBI a jeho neustálého zlepšování. Tento závazek je základním předpokladem pro zavedení a fungování celého systému SŘBI a pro zajištění bezpečnosti informací.

Zdroje zajišťující provoz SŘBI a informačních systémů LK, jsou plně v odpovědnosti vedení LK a krajského úřadu. Je nezbytné, aby tyto zdroje byly adekvátně vyžadovány, řízeny a jejich využití bylo plánováno s dostatečným předstihem a plně pokrývalo potřeby LK a krajského úřadu, a to v souladu s  rozpočtem LK na jednotlivé oblasti.

Vedení LK a vedení krajského úřadu poskytuje zdroje potřebné pro:

* vybudování, zavedení, provoz, monitorování, udržování a zlepšování SŘBI,
* udržování souladu se zákonnými a dalšími požadavky a dodržování bezpečnostních závazků, uvedených ve smlouvách,
* udržování odpovídajících opatření,
* provedení přezkoumání systémů bezpečnosti podle potřeby a zajištění odpovídajících reakcí na jejich výsledky.

Jednotlivé požadavky na zdroje k zajištění bezpečnosti jsou formulovány jednotlivými garanty IS a vedoucími odborů a oddělení v listinné či elektronické formě a s dostatečným předstihem. Z  požadavků by mělo být zcela jasné vymezení a zdůvodnění potřebných zdrojů. Návrhy jsou doručovány MKB, který tyto návrhy předloží na VŘKB a ten následně rozhodne o dalších krocích.

Zejména se jedná o následující zdroje:

* **Personální zdroje** pro výkon nezbytných činností (rolí) v SŘBI ve stanovené organizační struktuře,
* **Finanční zdroje** pro nákup nezbytných technologií a služeb a k provozování SŘBI,
* **Technické zdroje** pro implementaci bezpečnostních opatření v provozovaném SŘBI.

## Bezpečnost informací v řízení projektů

Bezpečnost informací musí být začleněna do metodiky (metodik) řízení projektů. Projektem se rozumí časově ohraničená a ucelená sada činností a procesů, jejímž cílem je zavedení, vytvoření nebo změna něčeho konkrétního. Musí mít jasný cíl, výsledek či užitek, tedy něco, co se má realizovat, vytvořit či změnit. V prostředí LK a krajského úřadu, je cílem zajistit, že jsou identifikována rizika bezpečnosti informací a jsou řešena jako součást projektu. To platí pro projekty, jejichž povaha a financování může ovlivnit bezpečnost informací, například projekt nové poskytované služby v oblasti ICT, nákupu a servisu ICT, správy zařízení a dalších podpůrných procesů.

Používané metody řízení projektů musí vyžadovat, aby:

* cíle bezpečnosti informací byly zahrnuty do projektových cílů;
* posuzování rizik bezpečnosti informací probíhalo již v rané fázi projektu a aby byla identifikována nezbytná opatření,
* bezpečnost informací byla součástí všech fází použité projektové metodiky, která musí obsahovat alespoň následující kroky v jednotlivých etapách projektu:
	+ Definice předmětu projektu – definice bezpečnostních cílů
	+ Analýza předmětu – stanovení přesných bezpečnostních požadavků
	+ Realizace projektu – požadavky na:
		- Bezpečnost vývojového prostředí
		- Bezpečnost vývoje
		- Bezpečnostní testování
	+ Implementace/nasazení produktu – kontrola splnění bezpečnostních požadavků
	+ Ukončení projektu – Vyhodnocení bezpečnostních opatření

Dopady na bezpečnost informací musí být řešeny a pravidelně přezkoumávány ve všech projektech dle postupů a odpovědností za bezpečnost informací, které jsou definovány v příloze č. 3 - Politika řízení dodavatelů.

## Pravidla a postupy pro provádění auditů

Audit systému řízení bezpečnosti informací ověřuje správnost a účinnost zavedených bezpečnostních opatření a jejich shodu s právními předpisy, organizačními směrnicemi, jinými předpisy a smluvními závazky.

VŘKB zadá audity SŘBI v naplánovaných intervalech nebo dle potřeby a na vyžádání od Rady nebo vedení krajského úřadu.

VŘKB schvaluje audity na základě podkladů MKB uvedených v dokumentu Roční program auditů.

Auditor kybernetické bezpečnosti provádí audit v následných krocích:

* plánování auditu,
* provedení auditu a sběr důkazů o prováděných činnostech,
* vyhodnocení auditu, v rámci kterého jsou jednotlivá zjištění ohodnocena a auditovaný subjekt je seznámen s výsledky,
* vypracování zprávy z auditu.

Auditor kybernetické bezpečnosti předloží zprávu ke schválení řediteli úřadu a VŘKB. Na základě výsledků auditu MKB stanoví opatření k odstranění nedostatků.

Výsledky auditů jsou pravidelně vyhodnocovány a na základě zjištění z auditu jsou přijímána opatření ke zlepšení systému řízení bezpečnosti informací. Program auditů je případně doplněn o mimořádné audity s cílem ověřit efektivitu nápravných opatření z předchozích auditů.

Roli Auditora kybernetické bezpečnosti je možné zajistit činnostmi Interního auditu krajského úřadu. Pokud nemají zaměstnanci oddělení interního auditu adekvátní (dostatečné, příslušné) odborné znalosti a zkušenosti (a dovednosti), budou nezbytné auditorské služby zajištěny externě. O každém zadání auditu rozhodne VŘKB.

## Pravidla a postupy pro nápravná opatření a zlepšování systému řízení bezpečnosti informací

Pravidla a postupy pro nápravná opatření vyplývajících z auditních šetření jsou specifikována v příloze 21 této směrnice - Politika pro zvládání kybernetických bezpečnostních incidentů.

# Závěrečná ustanovení

1. Tato směrnice byla schválena Radou Libereckého kraje dne 23. 04. 2019, usnesením
č. 788/19/RK a zrušuje Směrnici Rady kraje č. 4/2018.

 V Liberci dne 30. 04. 2019

 Martin Půta

 Hejtman