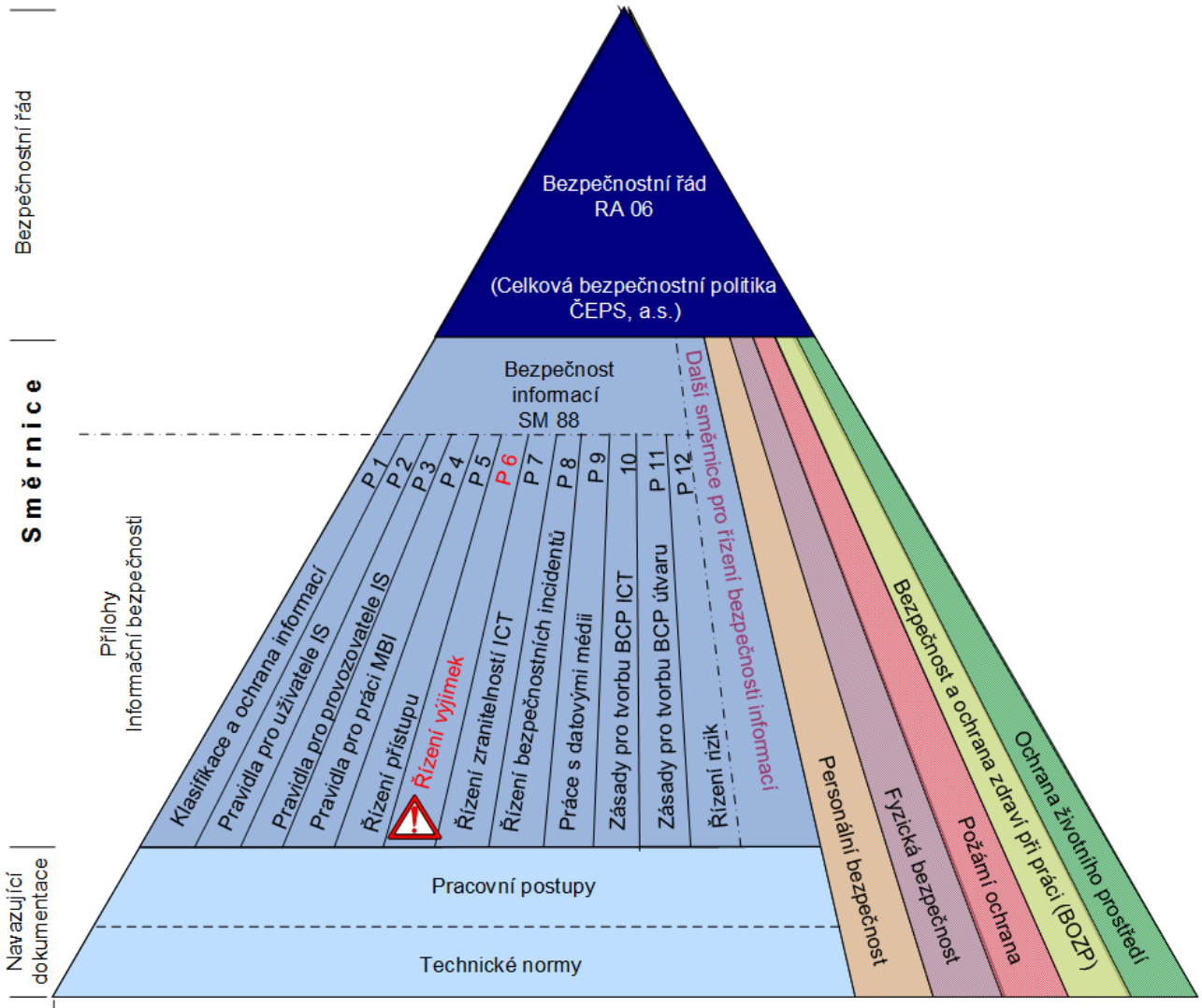
ŘÍZENÍ VÝJIMEK BEZPEČNOSTI INFORMACÍ

Zařazení a působnost dokumentu ve struktuře bezpečnostní dokumentace



dokument / působnost	Klasifikace a ochrana informací	Pravidla pro uživatele IS	Pravidla pro provozovatele IS	Pravidla pro práci MBI	Řízení přístupu	Řízení výjimek	Řízení zranitelností ICT	Řízení bezp. incidentů	Práce s datovými médii	Zásady pro tvorbu BCP ICT	Zásady pro tvorbu BCP útvaru	Řízení rizik
uživatel IS	x	x										
provozovatel IS	x	x	x	x	x		x	x	x	x		x
MBI	x	x		x	x	x	x	x	x	x	x	x
vedoucí útvaru	x	x									x	x
personalista	x	x			x							
externí subjekt	x	x	x*)		x*)							

*) *Platí pro externí subjekty v roli správců/administrátorů/vývojářů IS*

Pozn.: Uvedené názvy nejsou přesnými názvy příloh.

OBSAH:

1 ÚČEL, PŮSOBNOST A ODPOVĚDNOST

Dokument *Řízení výjimek bezpečnosti informací* je samostatnou přílohou směrnice *Bezpečnost informací* (dále „SM/88“) stanovující základní principy, pravidla a požadavky bezpečnosti informací. Tato příloha definuje základní proces, odpovědnosti a pravomoci pro schvalování bezpečnostních výjimek a s tím související akceptaci rizik, která mohou pro společnost z výjimky vyplynout.

1.1 Role, odpovědnosti a pravomoci

Žadatel o udělení bezpečnostní výjimky je kterýkoliv uživatel či správce informačního systému a je odpovědný za:

- vyplnění žádosti o udělení výjimky,
- doplnění podkladů žádosti o udělení výjimky, pokud je vyžadováno,
- včasné požádání o prodloužení výjimky,
- uvedení bezpečnostních opatření do souladu se standardy společnosti po ukončení platnosti výjimky (požadovaná úroveň bezpečnosti musí být žadatelem zajištěna před ukončením platnosti výjimky).

Přímý nadřízený žadatele odpovídá za schválení nebo zamítnutí žádosti o udělení výjimky (posuzuje, zda je výjimka nutná pro plnění pracovních povinností).

Specialista bezpečnosti informací je zaměstnanec oddělení Strategie a bezpečnost ICT odpovědný za:

- provádění hodnocení rizik,
- návrh opatření pro eliminaci rizik, nebo kompenzačních opatření v případě akceptace rizik.

Manažer bezpečnosti informací (MBI) řídí udělování výjimek:

- převzetí schválené žádosti,
- zajištění posudku realizovatelnosti,
- zajištění procesu posouzení rizik,
- doporučení k akceptaci rizik,
- postoupení akceptace rizika odpovědné osobě,
- udělení výjimky (na základě schválení odpovědnou osobou),
- pravidelné revize udělených výjimek,
- evidenci udělených výjimek.

Odpovědná osoba je vedoucí útvaru, jehož se výjimka týká (včetně ředitelů sekcí EŘIS, ICT služby, Řízení provozu a údržby a manažera informační bezpečnosti). Odpovědná osoba provádí:

- akceptaci rizik, která jsou výjimkou způsobena nebo ovlivněna,
- schválení výjimky.

Ředitelé sekcí EŘIS, ICT služby a Řízení provozu a údržby jsou v roli odpovědné osoby a dále provádějí:

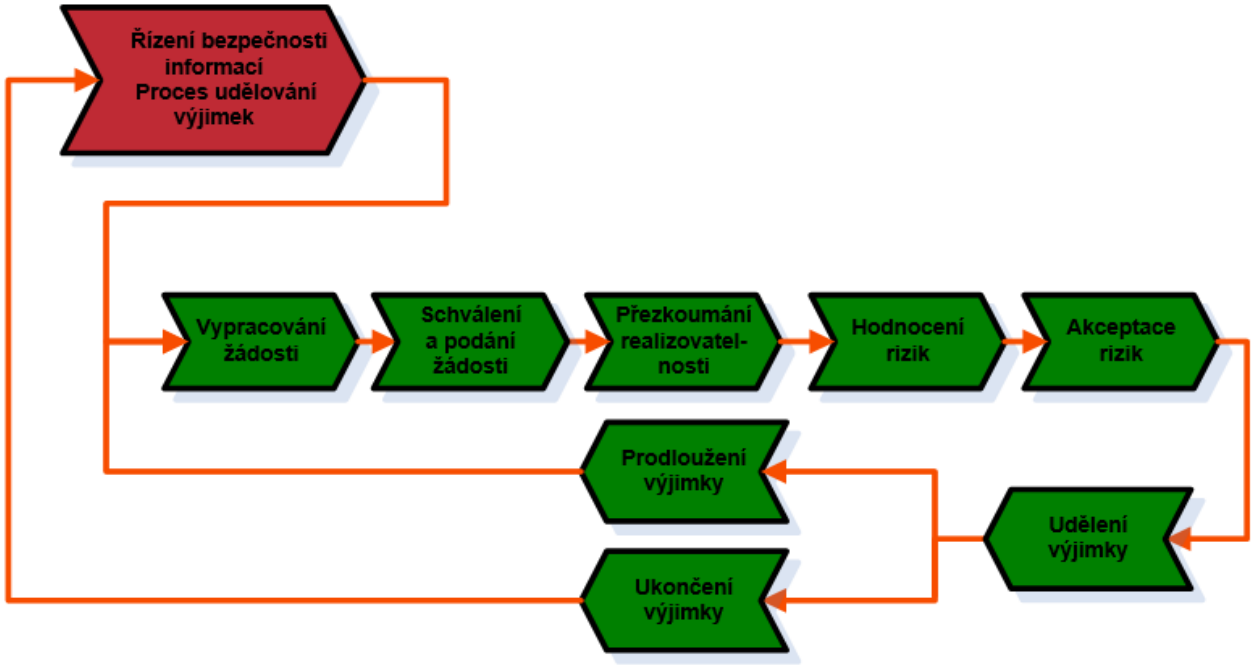
- posouzení realizovatelnosti výjimky,
- posouzení souladu se strategií ICT.

2 ŘÍZENÍ VÝJIMEK BEZPEČNOSTI INFORMACÍ

Výjimkou z bezpečnosti informací se rozumí odchylka od pravidel a postupů uvedených ve směrnici SM/88 a v jejích přílohách. Řízení výjimek bezpečnosti informací je součástí řízení bezpečnosti informací ČEPS. Proces se skládá z činností:

- vypracování žádosti o výjimku,
- schválení žádosti o výjimku,
- přezkoumání realizovatelnosti výjimky,

- hodnocení rizik, která z výjimky vyplývají pro ČEPS,
- schválení výjimky a akceptace souvisejících rizik,
- ukončení nebo prodloužení výjimky.



Obrázek 1. Proces řízení výjimek bezpečnosti informací

2.1 Vypracování žádosti o výjimku

Žádost o výjimku bezpečnosti informací vypracovává uživatel nebo správce informačního systému formou požadavku na HelpDesk ICT (kap. 4). V žádosti musí být uvedeno zejména:

- jméno, příjmení a kontaktní údaje (útvar, telefon a emailová adresa) žadatele,
- počátek a konec platnosti výjimky,
- věcný popis výjimky,
- odvolání na pravidlo nebo postup směrnice SM/88 nebo jejích příloh, ze kterého má být udělena výjimka.

2.2 Schválení žádosti o výjimku

Žadatel o výjimku předkládá žádost ke schválení svému přímému nadřízenému zaměstnanci. Skutečnost, že výjimka byla schválena, se uvede v žádosti, včetně kontaktních údajů schvalovatele. Po schválení zadá žadatel požadavek o udělení výjimky do HelpDesku ICT a vypracovanou žádost přiloží k požadavku. Specialista HelpDesku vyhodnotí požadavek a v případě, že se jedná o žádost o výjimku bezpečnosti informací se všemi náležitostmi, předá požadavek prostřednictvím workflow HelpDesku manažeru bezpečnosti informací k přezkoumání realizovatelnosti výjimky a k hodnocení rizik.

2.3 Přezkoumání realizovatelnosti výjimky

Pro schválení nebo zamítnutí výjimky bezpečnosti informací je nutné posouzení, zda je výjimka realizovatelná[1] po technické, procesní a případně i právní stránce.
Odborné posouzení realizovatelnosti zajišťují správci ICT ve spolupráci s jinými organizačními jednotkami, jejichž vyjádření k výjimce je nutné, a kterých se výjimka může dotýkat.
Není-li výjimka realizovatelná, je žádost o ni manažerem bezpečnosti informací zamítnuta a žadatel o výjimku je povinen odstranit příčinu, pro kterou výjimku žádal. O zamítnutí a jeho důvodech je žadatel informován.

2.4 Hodnocení rizik

V případech, kdy je výjimka realizovatelná, MIB zajistí ohodnocení rizik, které obvykle provádějí specialisté bezpečnosti informací. Podle jeho výsledku rozhodne o potřebě akceptace souvisejících rizik odpovědnou osobou a poskytne jí doporučení ke schválení nebo neschválení výjimky v procesu akceptace rizik.

2.5 Akceptace rizik

Akceptaci rizika provede odpovědná osoba, jejíž organizační jednotky nebo svěřených procesů[2] se rizika nejvíce dotýkají. Akceptaci rizik nemůže odpovědná osoba delegovat na podřízené.
Pokud nejsou odpovědnou osobou rizika akceptována, nesmí být výjimka udělena. Žadatel je povinen uvést věci, pro které o výjimku žádal, do standardního stavu nebo upraví standardní stav tak, že není třeba výjimku udělovat.

2.6 Udělení výjimky

Výjimku v oblasti bezpečnosti informací uděluje manažer bezpečnosti informací. Může tak učinit pouze v případě, že odpovědná osoba akceptuje rizika, která výjimka vyvolává. Současně s udělením výjimky MIB vždy určí podmínky, za kterých výjimka platí, nebo podmínky, za kterých výjimka pozbývá platnosti.
Výjimka se uděluje vždy na dobu určitou. V této lhůtě je žadatel povinen uvést věci, pro které o výjimku žádal, do standardního stavu nebo upraví standardní stav tak, že není třeba výjimku udělovat.

2.7 Prodloužení nebo ukončení výjimky

Výjimka, která byla udělena, může být prodloužena jen v odůvodněných případech. Proces prodloužení platnosti výjimky je shodný s procesem jejího udělení včetně nového ohodnocení a akceptace rizik. O prodloužení je nutné požádat před ukončením platnosti udělené výjimky. **Platnost výjimky může být prodloužena nejdéle na dobu jednoho roku.**
Pokud není platnost výjimky prodloužena, je žadatel povinen bez prodlení zajistit uvedení bezpečnostních opatření do souladu se směrnicí SM/88 a jejími přílohami nebo upraví standardní stav tak, že není třeba výjimku prodlužovat.

---

[1] Výjimka může nejen reprezentovat určitý aktuální stav, který je v rozporu s pravidly bezpečnosti, ale také může vyžadovat realizaci konkrétních změn, k jejichž realizovatelnosti se odborní posuzovatelé vyjadřují.
2 Svěřené procesy viz RA 02 *Organizační řád*

3 ZRYCHLENÝ PROCES UDĚLENÍ VÝJIMKY

V případě naléhavé situace je možné provést zrychlené udělení výjimky.
Zrychlené udělení výjimky je v kompetenci manažera bezpečnosti informací a může být provedeno za následujících podmínek:

- žádost o výjimku je schválena nadřízeným žadatele,
- žádost o výjimku je projednána se správci ICT,
- hodnocení výjimky potvrdí realizovatelnost a neindikuje vysoké riziko pro ČEPS,
- platnost výjimky bude omezená na období 1 měsíce a v případě nutnosti výjimku zachovat, projde tato standardním schválením a akceptací rizik.

4 NÁLEŽITOSTI ŽÁDOSTI O UDĚLENÍ VÝJIMKY BEZPEČNOSTI INFORMACÍ

Žádost o udělení výjimky bezpečnosti informací musí obsahovat:

Část 1 – vyplňuje žadatel

Jméno a příjmení, kontaktní údaje (tel., e-mail)

Datum vystavení žádosti

Popis výjimky vzhledem k zásadám bezpečnosti informací

Důvod pro udělení výjimky

Časové období pro udělení výjimky

souhlas přímého nadřízeného.

Část 2 – zajišťuje ředitel příslušné sekce ICT

Posouzení realizovatelnosti.

Část 3 – zajišťuje MIB

Ohodnocení rizik specialistou bezpečnosti informací

Rozhodnutí na základě hodnocení rizik (schválení výjimky, zamítnutí výjimky nebo předání odpovědné osobě k akceptaci rizik).

Část 4 – zajišťuje odpovědná osoba

Písemné prohlášení o akceptaci zjištěných rizik a odpovědnosti za jejich následky, schválení výjimky.

Část 5 – zajišťuje MIB

Udělení výjimky, které obsahuje:

- Datum počátku a ukončení platnosti
- Podmínky, při kterých výjimka pozbývá platnosti.