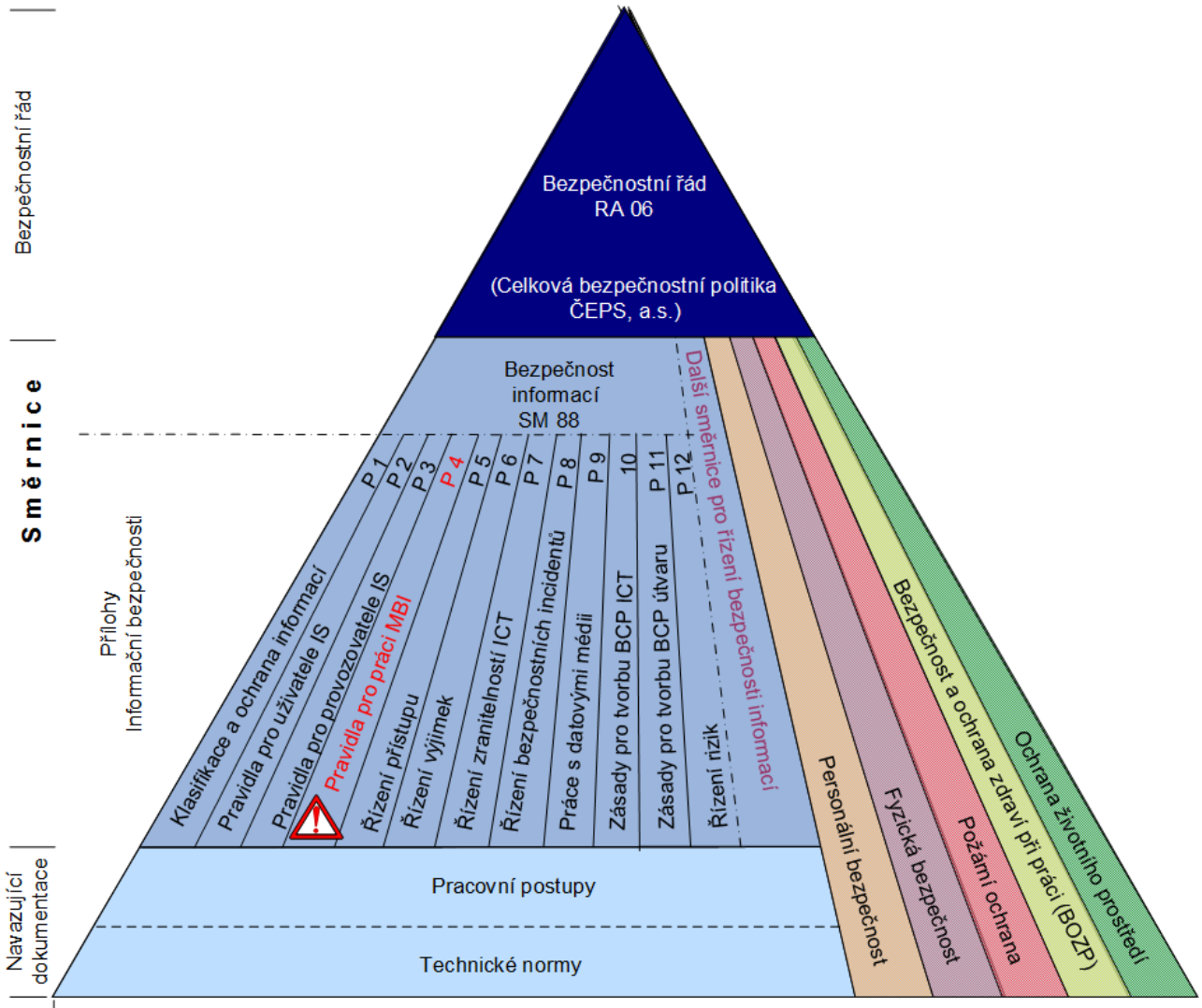
PRAVIDLA PRÁCE MANAŽERA BEZPEČNOSTI INFORMACÍ

Zařazení a působnost 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 A PŮSOBNOST

Dokument „*Pravidla práce manažera bezpečnosti informací"* je samostatnou přílohou směrnice *Bezpečnost informací* (dále „SM/88"), která stanovuje základní principy, pravidla a požadavky pro zajištění bezpečnosti informací v ČEPS. Tato příloha specifikuje činnosti, které manažer bezpečnosti informací (dále také „MBI") provádí nebo zajišťuje v oblasti řízení bezpečnosti informací.
Příloha je závazná pro MBI, provozovatele IS (sekci Energetické řídící a informační systémy, sekci ICT služby a sekci Řízení provozu a údržby) a pro oddělení Strategie a bezpečnost ICT. Informativní je pro všechny zaměstnance.

1.1 Role, odpovědnosti a pravomoci

Předpokladem pro zajištění bezpečnosti informací je její jednotné a soustavné prosazování a řízení. MBI je odpovědný za koordinaci veškerých činností nezbytných pro zajištění bezpečnosti informací ve společnosti.

Manažer bezpečnosti informací (MBI)

- odpovídá za navrhování koncepce bezpečnosti ICT služeb a zabezpečení ICT aktiv,
- řídí bezpečnostní radu ICT,
- odpovídá za stanovení doby uchování log záznamu dle jejich povahy a procesní/legislativní klasifikace,
- odpovídá za bezpečnost záznamů o informačních bezpečnostních incidentech a jejich archivaci,
- odpovídá za komunikaci s top-managementem o příčinách a dopadech aktuálních informačních bezpečnostních incidentů,
- odpovídá za informování koncových uživatelů o dopadech aktuálních informačních bezpečnostních incidentů a jejich nezbytné součinnosti.

MBI má právo vyžadovat součinnost od ostatních útvarů při činnostech souvisejících s řízením bezpečnosti informací MBI deleguje některé povinnosti na specialisty oddělení Strategie a bezpečnost ICT.

2 PRAVIDLA PRÁCE MANAŽERA BEZPEČNOSTI INFORMACÍ

2.1 Koncepční činnost

Bezpečnostní dokumentace

Základními dokumenty řízení bezpečnosti informací v ČEPS jsou RA 06 *Bezpečnostní řád* a směrnice SM/88 *Bezpečnost informací*.

MBI je odpovědný za návrh, koncepci a prosazování bezpečnosti informací v ČEPS. Vytváří komplexní strukturu dokumentace pro oblast bezpečnosti informací, koordinuje její tvorbu a aktualizace v periodě nepřekračující dva roky nebo dříve při významné změně v infrastruktuře ICT. Směrnice SM/88 musí zahrnovat:

- pravidla pro nakládání s informacemi (včetně klasifikace informací),
- pravidla bezpečnosti informací pro uživatele IS,
- pravidla bezpečnosti informací pro provozovatele a administrátora IS,
- pravidla pro řízení bezpečnostních incidentů,
- pravidla pro řízení zranitelností ICT,
- pravidla pro řízení bezpečnostních výjimek,

- pravidla pro práci s datovými médii,
- pravidla pro řízení přístupu k informacím a informačním systémům,
- zásady pro tvorbu plánů kontinuity a obnovy ICT,
- doporučené zásady pro tvorbu plánů kontinuity a obnovy činností útvaru
- řízení rizik bezpečnosti informací.

MBI spolupracuje s provozovateli IS při zpracovávání navazující technické dokumentace (např. konfigurační standardy systémů a zařízení ICT, zálohovací postupy, plány obnovy kontinuity ICT, plány údržby systémů apod.). MBI má právo a povinnost vyjadřovat se ke všem směrnicím, interním dokumentům a projektům, které se týkají bezpečnosti informací a informačních aktiv.

Rozvoj bezpečnosti informací

MBI se podílí na zvyšování úrovně bezpečnosti informací činnostmi:

- připravuje, řeší, schvaluje, koordinuje a kontroluje projekty bezpečnosti informací ve společnosti,
- spolupracuje s Risk manažerem při identifikaci rizik a navrhuje opatření k minimalizaci ICT rizik pro společnost v návaznosti na provedené analýzy rizik,
- zajišťuje součinnost s externími subjekty v oblasti zajištění bezpečnosti informací,
- připravuje metodiku BCM/BCP za oblast bezpečnosti informací.

Soulad s právními normami a technickými požadavky

MBI spolupracuje s právní službou, odborem Interní audit a s bezpečnostním ředitelem na sledování legislativních změn nebo změn předpisů závazných pro společnost a odpovídá za dodržování souladu bezpečnosti informací s obecně závaznými právními předpisy.

MBI sleduje technické požadavky na zajištění bezpečnosti informací (např. posuzuje kvalitu šifrovacích nástrojů, systémů řízení zranitelností, antivirových systémů apod.) a v případě potřeby vyvolává procesy, které vedou k jejich změně.

2.2 Analytická činnost

Analýza rizik a klasifikace informací

Analýza rizik (AR) je základním nástrojem pro posouzení ochrany informací společnosti. Při stanovení termínu a rozsahu analýzy rizik spolupracuje s řediteli příslušných sekcí. AR hodnotí rizika s ohledem na porušení základních kritérií bezpečnosti informací - **důvěrnosti, dostupnosti, integrity** a případně **nepopiratelnosti** informačních aktiv.

Výstupem AR je návrh opatření pro eliminaci identifikovaných rizik zpracovaný v Plánu zvládání rizik (RTP). Výsledky AR spolu s vyjádřením ředitelů příslušných sekcí MBI předkládá vedení společnosti, které rozhodne o realizaci nápravných opatření nebo o akceptaci zbytkových rizik.

MBI odpovídá za zajištění klasifikace a ochrany informací na základě výsledků analýzy rizik informačních systémů (etapa identifikace informačních aktiv). Proces práce s klasifikovanými informacemi (označování, předávání, ukládání i likvidace) je popsán v Příloze č. 1 SM/88 a MBI odpovídá za její dodržování.

Pořízení, vývoj a provoz informačních systémů

MBI má právo a povinnost vyjadřovat se v rámci procesu řízení změn v ICT k nově pořizovaným a nasazovaným softwarovým i hardwarovým systémům, které posuzuje z hlediska bezpečnosti informací. Jedná se zejména o způsob autentizace a autorizace uživatelů, kvalitu hesel, nastavení

přístupových práv, zabezpečení síťové komunikace, řešení vzdálených přístupů a připojování mobilních zařízení do vnitřní sítě, možnosti monitoringu a logování, zálohování dat apod. Implementaci do provozního prostředí realizují sekce Energetické řídící a informační systémy nebo ICT služby nebo úsek Provoz a správa majetku.

Nákup programového vybavení a zařízení ICT

MBI ve spolupráci s příslušným uživatelem a provozovateli ICT specifikuje požadavky bezpečnosti informací pro výběr nového SW nebo zařízení ICT. Posouzen musí být vliv na stávající informační aktiva a na úroveň zabezpečení klasifikovaných informačních aktiv. V kompetenci MBI je především schválení šifrovacích prostředků, dohledových bezpečnostních systémů a systémů pro řízení zranitelností, antivirových nástrojů apod.

Specifikace vyvíjeného software

MBI ve spolupráci s příslušným uživatelem a provozovateli ICT specifikuje požadavky bezpečnosti informací pro interní nebo externí vývoj nového SW a kontroluje jejich plnění v průběhu vývoje. Posouzen musí být vliv nového SW na zabezpečení informačních aktiv. Dokumentaci popisující řešení bezpečnostních požadavků schvaluje MBI.

Převzetí do provozu

MBI spolupracuje s provozovateli ICT na otestování účinnosti bezpečnostních mechanismů nového programového vybavení. Po splnění bezpečnostních požadavků stanovených zadávací specifikací schvaluje z pohledu bezpečnosti informací uvedení zakoupeného nebo vyvinutého softwaru do provozu.

Outsourcing a smluvní vztah s externími subjekty

Požadavky na bezpečnost informací musí splňovat smluvní vztahy s externími subjekty a s poskytovateli outsourcingu. MBI se za oblast bezpečnosti informací ke smluvní dokumentaci vyjadřuje. Sekce Nákup poskytuje manažeru bezpečnosti informací odpovídající části smluv k posouzení.

Pro zajištění bezpečnosti musí smlouva obsahovat alespoň:

- závazek dodržovat legislativu země,
- souhlas s bezpečnostními požadavky např. na bezpečnostní audit a testování poskytované služby odběratelem nebo jiným externím subjektem,
- souhlas s dodržováním relevantních interních předpisů ČEPS,
- definici prostředků pro zabezpečení vzájemné komunikace (např. úroveň šifrování),
- definici kontrolních mechanismů a metrik pro ohodnocení poskytované služby (SLA),
- dohodu o mlčenlivosti (NDA),
- definici vlastnických a autorských práv k poskytované službě nebo dílu a souhlas vlastníků těchto práv pro použití služby nebo díla v ČEPS,
- stanovení míry ručení a závazků v případě škody způsobené poskytovatelem služby.

Po dobu trvání smluvního vztahu musí být plnění bezpečnostních požadavků pravidelně kontrolováno. Vlastnosti monitoringu určuje MBI a pořizuje o něm záznamy.

2.3 Reaktivní činnost

Reaktivní činnosti jsou:

- detekce, vyhodnocování a zvládání bezpečnostních incidentů,
- řešení mimořádných událostí.

Řízení a řešení bezpečnostních incidentů

Procesem zvládání bezpečnostních incidentů se zabývá Příloha č. 8 SM/88. Definuje postupy pro účinnou a efektivní reakci na bezpečnostní incidenty. Cílem je minimalizace negativních dopadů na chod společnosti a prevence opakování incidentů.

Úloha MBI při detekci, vyhodnocování a zvládání incidentů bezpečnosti informací:

- v roli Klíčového uživatele řídí proces a technologie pro automatizované vyhodnocování bezpečnostních událostí z IT systémů (SIEM), jeho rozvoj a provoz,
- koordinuje činnost ostatních útvaru při vyhodnocování detekovaných bezpečnostních událostí a ukládá administrátorům nezbytné úkoly,
- řídí proces zvládání závažných bezpečnostních incidentů, spolupracuje s provozovateli ICT při rozhodování o postupu řešení,
- svolává řešitelský tým (Information Security Incident Response Team) a koordinuje jeho činnost,
- řídí zajišťování důkazního materiálu,
- vyjadřuje se k řešení incidentů bezpečnosti informací provozovateli IS,
- analyzuje bezpečnostní incidenty a koordinuje práci při implementaci schválených nápravných opatření,
- vede evidenci bezpečnostních událostí a incidentů v databázích HelpDesků jednotlivých IS,
- v součinnosti s provozovateli ICT vyhodnocuje statistiky o incidentech bezpečnosti informací a předkládá je vedení společnosti,
- v souladu s požadavky zákona o kybernetické bezpečnosti zajišťuje komunikaci s Národním bezpečnostním úřadem (NBÚ) týkající se bezpečnostních incidentů.

MBI je oprávněn při řešení bezpečnostních incidentů využívat i restriktivních nástrojů (např. iniciovat zablokování uživatelského účtu, odebrání přístupových práv k systému nebo aplikaci, došlo-li k podezření nebo ke zjištění porušení pravidel informační bezpečnosti).

MBI předkládá Bezpečnostní radě ICT přehled nejzávažnějších incidentů a zprávu o jejich řešení.

Každý závažný bezpečnostní incident kategorie 2 nebo 3 (viz Příloha č. 8 SM/88 *Řízení bezpečnostních incidentů)* musí být podnětem pro zamezení jeho opakování a pro zavedení opatření vedoucích ke zlepšení bezpečnosti informací. MBI vyhodnocuje návrhy na zlepšení bezpečnosti informací ve společnosti. O realizaci opatření musí být vždy informován jeho navrhovatel.

Řízení kontinuity činností (BCM)

MBI v procesu řízení kontinuity ICT:

- iniciuje provedení analýzy dopadu (BIA),
- iniciuje a kontroluje tvorbu, aktualizaci i pravidelné testování systému havarijních plánů (BCP) a plánů obnovy (DRP),
- vyjadřuje se k připraveným havarijním plánům a plánům obnovy,
- kontroluje ověření funkčnosti implementovaných bezpečnostních opatření IS/IT po haváriích a závažných bezpečnostních incidentech,
- kontroluje dokumentaci BCM.

Udělování výjimek

MBI řídí proces udělování výjimek z pravidel bezpečnosti informací. Stav bezpečnosti informací, který řízeně[1] neodpovídá směrnici SM/88 a navazující dokumentaci (např. přidělování nestandardních práv nebo nestandardních požadavků na hesla, schválení provozu atypických aplikací, povolování vzdálených přístupů externích subjektů apod.), musí být veden jako výjimka s akceptací souvisejících rizik.

Proces udělování výjimek bezpečnosti informací je popsán v Příloze č. 6 SM/88.

2.4 Kontrolní a preventivní činnost

MBI musí být informován o významných změnách v ICT ČEPS prostřednictvím procesu řízení změn v ICT a musí mu být poskytnuta dokumentace pro posouzení bezpečnostních dopadů.

MBI iniciuje, koordinuje nebo zajišťuje:

- provádění technických auditů a penetračních testů, při jejich přípravě spolupracuje s ředitelem příslušné sekce ICT (s výjimkou předem neohlašovaných penetračních testů),
- spolupráci při provádění interního a externího auditu bezpečnosti ICT,
- připomínkování celkové bezpečnostní politiky společnosti (RA 06),
- kontrolu dodržování dokumentace bezpečnosti informací,
- kontrolu dodržování procesů bezpečnosti informací ve spolupráci se odborem Interní audit,
- provádění testů funkčnosti procesů BCP/DRP,
- řízení zranitelností IS/ICT (Příloha č. 7 SM/88),
- apod.

Monitoring

MBI navrhuje rozsah monitoringu a podmínky pro uchovávání záznamů (logů) v součinnosti se správci ICT, kteří monitoring provádějí. Rozsah monitoringu musí být v souladu s dokumentací bezpečnosti informací, s možnostmi aplikace nebo systému, s obecně závaznými právními předpisy a s ohledem na certifikační požadavky, výsledky analýzy rizik, nálezy externího či interního auditu, závěry z řešení bezpečnostních incidentů apod. O monitorování činností a aktivit uživatelů musí být uživatelé předem informováni.

MBI musí mít pro zajištění kontrolní činnosti a šetření bezpečnostních incidentů přístup:

- pro čtení, k monitorování informačních systémů a technologií,
- na vyžádání, k monitorování informačních systémů a technologií neumožňujících přístup pro čtení,
- k provozovaným bezpečnostním dohledovým systémům (např. bezpečnostní portály, systémy řízení zranitelností apod.).

Systémové logy musí být pravidelně kontrolovány a vyhodnocovány správci ICT. O výsledku kontroly musí být informován MBI.

[1] Nejedná se o bezpečnostní incident, ale o řízený proces s akceptovatelnou mírou rizika.

Patch management

MBI musí být informován o zásadách, funkčnosti a prostředcích pro nasazování bezpečnostních oprav na zařízeních ICT.

Plán a provádění kontrol

MBI ve spolupráci se správci ICT připravuje roční plán *pravidelných* kontrol. Po nasazení nové významné aplikace nebo IS, po obnově systému procesem DRP nebo po vyřešení závažného bezpečnostního incidentu, zásadní změně ICT infrastruktury, při aktuální hrozbě apod. organizuje *neplánované* kontroly (např. audity systémů nebo penetrační testy).

Kontroly organizuje MBI. Realizují je buď zaměstnanci ČEPS nebo pracovníci externího subjektu (především technické testy, penetrační testy, audity systémů). Musí se provádět tak, aby nedošlo k ohrožení provozu IS a hlavních obchodních procesů společnosti. O průběhu a výsledcích kontroly připravuje odpovědný pracovník provádějící kontrolu písemný zápis, který předá manažeru bezpečnosti informací.

MBI odpovídá za evidenci všech provedených kontrol a jejich výsledků i za schválení postupu při odstraňování zjištěných nedostatků. Jednou ročně tuto evidenci vyhodnocuje a s výsledkem seznámí Bezpečnostní radu ICT.

2.5 Vzdělávací činnost

MBI je odpovědný za obsah bezpečnostního školení, metodiku školení a za průběžné zvyšování úrovně povědomí o informační bezpečnosti u zaměstnanců. Cílem školení je seznámit uživatele IS ČEPS se zásadami bezpečnosti informací stanovenými SM/88 a navazujícími dokumenty, se základními bezpečnostními pravidly, které musí zaměstnanci dodržovat i s aktuálními bezpečnostními hrozbami. Školení je organizováno odborem Personalistika. Metodicky a odborně je vedeno manažerem bezpečnosti informací ve spolupráci s bezpečnostním ředitelem.

3 SOULAD S POŽADAVKY

MBI je povinen dodržovat obecně závazné právní předpisy. Musí dodržovat ustanovení této přílohy a pravidla i bezpečnostní opatření týkající se ochrany důležitých informací organizace, osobních údajů a ochrany duševního vlastnictví (autorská a patentová práva) definovaná interní dokumentací. Zároveň je povinen iniciovat pravidelné aktualizace SM/88 včetně jejích příloh tak, aby byly v souladu s legislativními a interními předpisy platném znění.