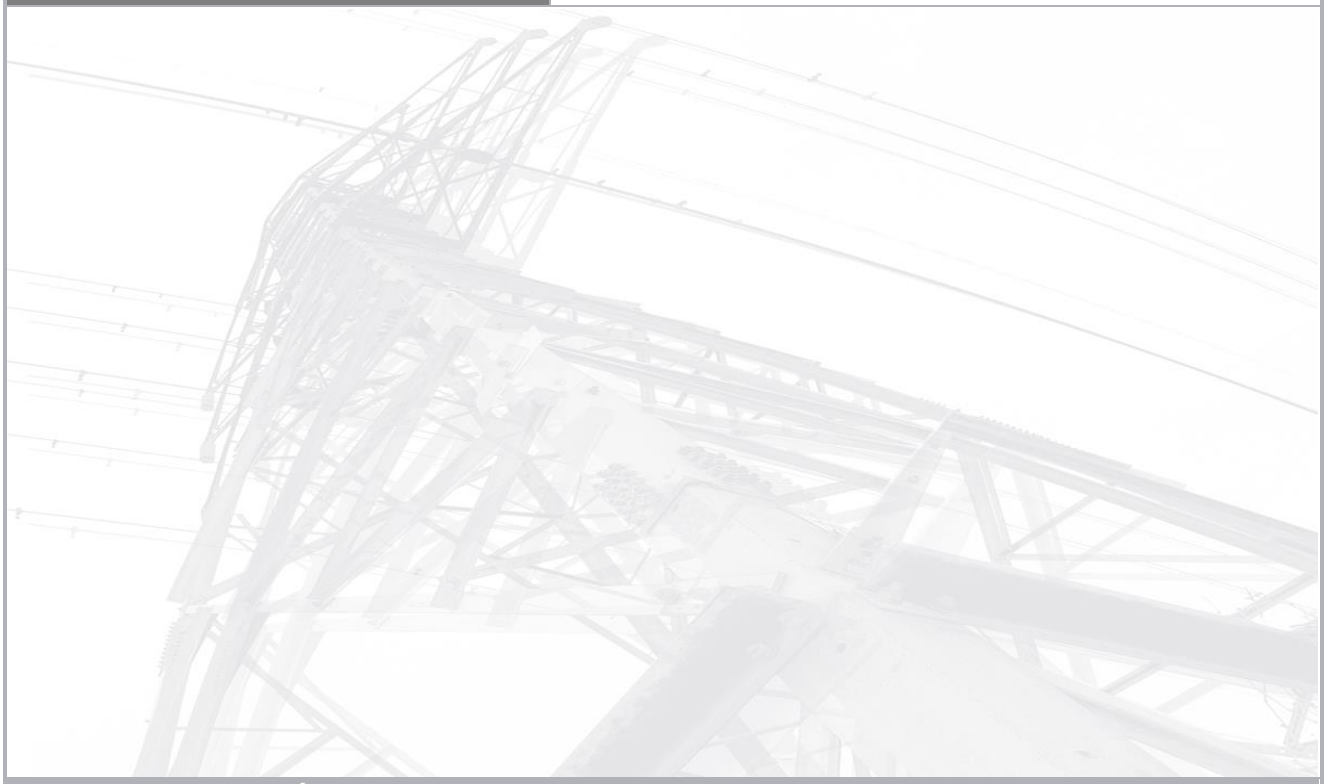
SMĚRNICE

Bezpečnost informací

SM/88/2016 **10. znění**	**Gestor:**	15000
	Útvar odpovídající za zpracování:	15002 Strategie a bezpečnost ICT
	Zpracovatel:	Ing. Jan Šmolík
Příslušnost k procesu	BR, ICT služby, ERIS, PC, PAU, SEM, RTK	



Platnost od:	Účinnost od:	Umístění	Schválil:
11. 10. 2016	11. 10. 2016	Intranet ČEPS	Ing. Jan Kalina předseda představenstva ČEPS, a.s. Ing. Miroslav Vrba, CSc. místopředseda představenstva ČEPS, a.s.

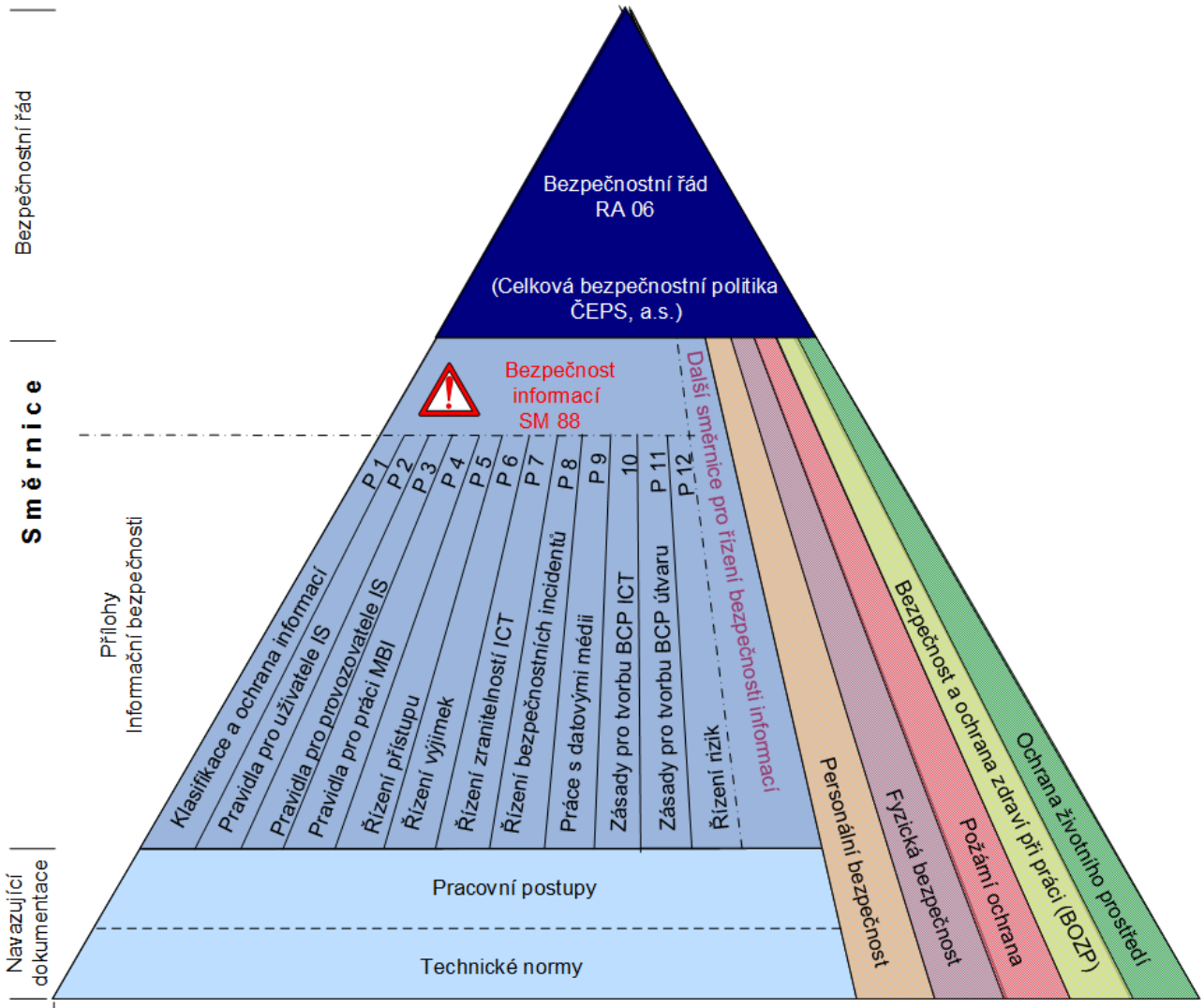
Popis změny:

10. znění přesunuje metodiku řízení rizik bezpečnosti informací obsaženou v původním znění směrnice do nové přílohy č. 12 a mění některou terminologii.

SM/88	**Bezpečnost informací**	10. znění

Historie změn		
Číslo znění	**Datum účinnosti**	**Popis změny**
4.	1. 1. 2013	Pravidelná aktualizace směrnice reflektující organizační změny a změna standardu BS 25999 na mezinárodní normy ISO 22301 a ISO 22313.
5.	1. 7. 2013	Vydání nové přílohy č. 11 Doporučené zásady pro vytvoření plánů kontinuity a obnovy činností útvaru.
6.	30. 9. 2014	Zavedení systému řízení informační bezpečnosti (ISMS) dle ISO/IEC 27001:2013, rozšíření působnosti o řídicí systémy stanic PS.
7.	1. 10. 2015	Platnost a účinnost Zákona č.181/2014 Sb. o kybernetické bezpečnosti, implementace bezpečnostního monitoringu SIEM – P8, P4 a průběžná aktualizace.
8.	24. 11. 2015	Rozšíření rozsahu ISMS o ČEPS Invest, a.s. Aktualizace se týká pouze SM/88, přílohy zůstávají beze změn.
9.	7. 6. 2016	Zohlednění změny v systemizaci ČEPS, a.s.
10.	11. 10. 2016	Přesun metodiky řízení rizik bezpečnosti informací obsaženou v původním znění do nové přílohy č. 12; změna terminologie (Informační bezpečnost -> bezpečnost 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 ÚVODNÍ USTANOVENÍ, DŮVOD VYDÁNÍ A ÚČEL

1.1 Úvodní ustanovení

Tato směrnice tvoří základní dokument systému řízení bezpečnosti informací (ISMS, Information Security Management System). ISMS je ustaven, implementován, udržován a neustále zlepšován v souladu s požadavky normy ISO/IEC 27001.
Směrnice bezpečnosti informací stanovuje principy, pravidla a požadavky v oblasti bezpečnosti informací a je součástí bezpečnostní dokumentace navazující na RA 06 *Bezpečnostní řád.*
Směrnice Bezpečnost informací je závazná pro všechny zaměstnance a spolupracující externí subjekty. Zaměstnanci jsou povinni seznámit se v rozsahu odpovídajícím jejich pracovním povinnostem i s uvedenou navazující dokumentací (přílohami) a dodržovat ji.
Porušení pravidel bezpečnosti informací se považuje za porušení povinností vyplývajících z pracovněprávních předpisů a vnitřních předpisů společnosti a vztahujících se k vykonávané práci.
Stav bezpečnosti informací, který řízeně neodpovídá pravidlům pro zajištění bezpečnosti informací uvedeným v této směrnici, musí být veden jako výjimka s omezenou dobou platnosti a s akceptací rizik plynoucích z této výjimky. Výjimka musí být schválena ředitelem sekce nebo členem představenstva, do jehož působnosti dopady rizika patří. Řízením bezpečnostních výjimek je pověřen manažer bezpečnosti informací (viz Příloha 6 SM/88).

1.2 Důvod vydání a účel

ČEPS je provozovatel přenosové soustavy a je povinen zajistit **bezpečný a spolehlivý přenos elektřiny** pro uživatele přenosové soustavy ČR i v rámci mezinárodní spolupráce. Vzhledem k předmětu podnikání je začleněn do evropské a národní kritické infrastruktury.

Informační systém ČEPS poskytuje informační podporu klíčovým procesům souvisejícím s hlavním předmětem podnikání společnosti. Ztráta informační podpory klíčových procesů nebo únik citlivých informací mohou vážně ohrozit kritickou infrastrukturu, podnikatelské aktivity a majetek společnosti.

1.3 Zajištění bezpečnosti informací

Vrcholové vedení společnosti tímto dokumentem vyjadřuje trvalou podporu prosazování bezpečnosti informací ve společnosti a prohlašuje, že:

- *podmínkou pro dosažení obchodních cílů společnosti je zajištění bezpečnosti informací a jejího neustálého zlepšování zaváděním přiměřených opatření, která budou chránit informační aktiva tak, aby poskytla odpovídající míru záruk našim zákazníkům, partnerům a akcionářům,*
- *základními zdroji pro řízení bezpečnosti informací v rámci společnosti jsou obecně závazné právní předpisy, standardy, normy a doporučení, které musí být v procesu řízení bezpečnosti informací respektovány,*
- *pojmem bezpečnost informací rozumíme proces zajišťování ochrany informací na potřebné úrovni z hlediska jejich důvěrnosti, dostupnosti a integrity.*

Vedení společnosti tímto dokumentem:

- *deklaruje svůj závazek k ustavení, implementaci, udržování a neustálému zlepšování systému řízení bezpečnosti informací (ISMS) a k zajištění zdrojů potřebných pro tento systém,*
- *deklaruje svůj závazek k zajištění stanovení cílů ISMS a plánu jejich dosažení,*
- *prosazuje požadavky a zásady bezpečnosti informací, které zajistí důvěrnost, integritu a dostupnost informací.*

1.4 Rozsah ISMS

Tato směrnice se vztahuje na práci s informacemi v působnosti rozsahu ISMS ve společnosti ČEPS a ČEPS Invest (v rámci poskytování SLA služeb společností ČEPS pro tuto společnost). Rozsah ISMS koresponduje s business modelem společnosti (BMS) ČEPS a organizační strukturou ČEPS Invest[1].

V následujících bodech je definován rozsah a hranice ISMS ČEPS a ČEPS Invest na základě posouzení specifických rysů činností těchto společností, jejich uspořádání, struktury, umístění (lokalit), aktiv a technologií.

1.4.1 Procesy a činnosti organizace

Rozsah ISMS se vztahuje na zpracování, uchovávání a distribuci informací v rámci všech procesů obou společností.

1.4.2 Lidské zdroje

Do působnosti ISMS náleží všichni zaměstnanci ČEPS a ČEPS Invest a pracovníci třetích stran (externích subjektů), vázaných smluvními vztahy, podílejících se na realizaci procesů zahrnutých do působnosti a rozsahu ISMS.
Řízení lidských zdrojů je upraveno organizační strukturou, která je ustanovena v platném organizačním řádu ČEPS a ČEPS Invest.

1.4.3 Informační aktiva

Rozsah ISMS pokrývá informační (datová) aktiva ČEPS a ČEPS Invest. Ohrožení jejich dostupnosti, důvěrnosti, integrity a nepopiratelnosti může narušit procesy těchto společností.
Informační aktiva jsou identifikována a ohodnocena ve zprávě o analýze dopadů a rizik.

1.4.4 Infrastruktura informačních systémů

V rozsahu ISMS jsou veškeré informační systémy zpracovávající informační aktiva zahrnutá do působnosti a rozsahu ISMS.
Infrastrukturu informačních systémů tvoří fyzická aktiva (především hardware ICT), programová aktiva (především aplikační a databázový SW), telekomunikační a další technické a podpůrné služby. Tato aktiva jsou evidována v dílčích registrech aktiv.
Pokud jsou informační systémy nebo jejich části outsourcovány, musí být prosazovány požadavky na bezpečnost informací pomocí smluvních ujednání s třetími stranami, které tyto služby poskytují.

1.4.5 Lokality/Budovy/Místnosti

Do působnosti ISMS náleží veškeré lokality, budovy a místnosti, ve kterých jsou uložena nebo provozována fyzická a informační aktiva, která jsou využívána v rámci procesů zahrnutých do působnosti a rozsahu ISMS.

1.4.6 Třetí strany a rozhraní ISMS

Procesy společnosti spadající do působnosti ISMS mohou být v některých případech závislé na službách (relevantních z hlediska bezpečnosti) poskytovaných třetími stranami. Pro tyto třetí strany

[1] Pokud je dále v textu použito spojení „rozsah ISMS“ má se na mysli rozsah ISMS společností ČEPS a ČEPS Invest.

musí existovat jasně formulované smlouvy a závazky mezi společností a touto organizací. Ve smlouvách musí být prosazeny požadavky na bezpečnost informací, včetně práva na provedení zákaznického auditu.

1.4.7 Vyjmutí z rozsahu ISMS

Do rozsahu ISMS nejsou zahrnuty utajované informace (včetně certifikovaných informačních systémů na jejich zpracování) vymezené a chráněné dle zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti.

2 DEFINICE ZÁKLADNÍCH POJMŮ A ZKRATEK

Aktivum - vše, co má pro společnost hodnotu; aktiva jsou **informační** (data a dokumenty), **programová** (aplikační a systémové vybavení), **fyzická** (počítačové a komunikační vybavení, média, prostory) a **služby** (počítačové, komunikační a servisní).

Autorizace přístupu k informacím - proces udělení (odepření) přístupu k informacím.

Bezpečnost informací - zachování **důvěrnosti** (ochrana před neautorizovaným přístupem, odhalením nebo aktivním odposlechem), **integrity** (správnost a úplnost) a **dostupnosti** (autorizovanému uživateli dle potřeby) informací a s nimi spojené priority např. autentičnost, odpovědnost, nepopiratelnost a spolehlivost.

Bezpečnostní incident - činnost nebo událost ohrožující informační aktiva nebo narušující bezpečnostní procedury. Bezpečnostní incident (informační) v kontextu ISMS je nutné odlišit od bezpečnostních incidentů v přenosové soustavě (provozních), v této politice a jejich přílohách je pojmem „bezpečnostní incident“ nebo „incident“ označován „incident bezpečnosti informací“.

Business Continuity Management (BCM) - řízení kontinuity podnikání.

ČEPS Invest - ČEPS Invest, a.s., IČO 24670111, se sídlem Elektrárenská 774/2, Michle, 101 00 Praha 10.

Garant (vlastník) aktiv – definovaná bezpečnostní role v souladu se zákonem o kybernetické bezpečnosti, představující fyzickou osobu, pověřenou k zajištění rozvoje, použití a bezpečnosti aktiva. Jde o obdobnou roli, jakou je vlastník aktiva podle řady norem ISO/IEC 27tis.

Hodnocení rizik – proces, při němž je určována významnost rizik a jejich přijatelná úroveň.

Hrozba - potencionální příčina kybernetické (nebo jiné) bezpečnostní události nebo kybernetického bezpečnostního incidentu, jejímž výsledkem může být poškození aktiva.

Informační systém (IS) - soustava infrastruktury, aplikací, organizačních opatření, procedur a souvisejících služeb pro tvorbu, získávání, zpracování, ukládání a prezentaci informací pro podnikatelské a řídící procesy.

ISMS – „Information Security Management System“ (systém řízení bezpečnosti informací). Systémem řízení bezpečnosti informací je část systému řízení založená na přístupu k rizikům významného informačního systému, která stanoví způsob ustavení, zavádění, provoz, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací.

Informační a komunikační technologie (ICT) - prostředky (zařízení, systémy, organizační opatření, dokumentace apod.) používané pro zpracování a přenos informací v elektronické formě. Pod pojmem IS/ICT se též rozumí Řídicí Systém stanic Přenosové Soustavy (dále ŘS stanic PS).

NBÚ – Národní bezpečnostní úřad.

Opatření nebo také bezpečnostní opatření - organizační, technický, řídící nebo legislativní prostředek pro řízení rizik.

Riziko - kombinace pravděpodobnosti, že dojde k nežádoucí události a následků, které mohou z takové události vzniknout.

Řízení rizik – činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik.

Řízení zranitelností (Vulnerability Management) - systémové řešení včasného vyhledání, otestování, hodnocení a odstranění zranitelností a chyb v nastavení ICT produktů.

SIEM – Security Information and Event Management (bezpečnostní monitoring)

Systém řízení bezpečnosti informací - systematický proces zajištění mechanismů, které umožní dosažení přiměřené úrovně bezpečnosti informací v čase (**ISMS** = **I**nformation **S**ecurity **M**anagement **S**ystem).

Uživatel IS - zaměstnanec s oprávněným přístupem k informačnímu systému.

ZoKB – zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

Zranitelnost - slabé místo aktiva nebo skupiny aktiv, které může být využito jednou nebo více hrozbami.

3 PŮSOBNOST A ODPOVĚDNOST

3.1 Působnost

Směrnice se vztahuje na práci s informacemi v působnosti všech procesů v rozsahu ISMS. Výjimkou jsou utajované informace ve smyslu zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

3.2 Role, odpovědnosti a pravomoci

Role, odpovědnosti a pravomoci vycházejí ze zásad stanovených bezpečnostním řádem.

Obecné role a odpovědnosti

Zaměstnanec je v rámci své působnosti povinen:

- seznámit se s interními předpisy bezpečnosti informací a dodržovat je,
- zajišťovat soustavnou ochranu informačních aktiv společnosti (zachování jejich důvěrnosti, dostupnosti a integrity),
- hlásit bezpečnostní incidenty a chování, která by mohla být bezpečnostním incidentem,
- předcházet vzniku událostí s dopadem na bezpečnost informací a aktivně postupovat při odhalování a likvidaci následků bezpečnostních incidentů,
- aktivně spolupracovat při analýzách rizik, při hodnocení stavu informační bezpečnosti a při bezpečnostních auditech,
- uplatňovat klasifikaci informací v souladu s Přílohou č. 1.

Zaměstnanec je oprávněn:

- vyžadovat plnění bezpečnostních standardů, zásad a opatření ve společnosti,
- vyžadovat odbornou a metodickou pomoc při řešení jeho požadavků a problémů v oblasti bezpečnosti informací od specialistů informační bezpečnosti.

Pravidla bezpečnosti informací pro uživatele informačních systémů podrobně specifikuje Příloha č. 2. Pravidla bezpečnosti informací pro provozovatele a administrátory informačních systémů jsou v Příloze č. 3.

Vedoucí zaměstnanec[2]:

- je v rámci své působnosti povinen vytvářet podmínky pro zajištění bezpečnosti informací a kontrolovat seznámení zaměstnanců s touto směrnicí a s navazující dokumentací.
- odpovídá za zajištění souladu jím řízených procesů nebo organizačních jednotek s touto směrnicí:
  - spolupracuje při zavádění opatření na ochranu informací a při zajištění kontinuity činností společnosti,
  - uplatňuje bezpečnostní zásady ve své řídící činnosti a dbá na jejich dodržování podřízenými zaměstnanci,
  - zajišťuje řízený přístup k informacím a systémům ve své kompetenci (schvalováním a revizí přístupových práv pro své podřízené),
  - sjednává ve smlouvách s externími subjekty požadavky bezpečnosti informací,
  - podílí se na řešení bezpečnostních incidentů ve své působnosti a z výsledků vyvozuje personální opatření u svých podřízených,
  - řeší krizové situace a havarijní stavy podle předem připravených plánů,
  - akceptuje rizika bezpečnosti informací spadající do jeho kompetence.

Vrcholový management:

- prosazuje bezpečnost ve společnosti podporou bezpečnostních aktivit a přidělováním odpovědností za bezpečnost,
- podporuje koordinaci při zavádění informační bezpečnosti ve všech organizačních jednotkách společnosti,
- zajišťuje kontinuitu činností,
- akceptuje rizika informační bezpečnosti spadající do jeho kompetence.

Zvláštní role a odpovědnosti

Představenstvo odpovídá v rámci své působnosti a v souladu s RA 06 za celkovou bezpečnost společnosti včetně bezpečnosti informací.

Člen představenstva pověřený řízením úseku *Dispečerské řízení a ICT*:

- řídí oblasti ICT a vytváří dostatečné zdroje tak, aby informační systémy ČEPS byly navrhovány, vyvíjeny i provozovány bezpečným způsobem a aby podporovaly plnění cílů společnosti s ohledem na existující rizika ve své působnosti,
- zajišťuje kontinuitu činností v celém rozsahu IS/ICT a požadovanou podporu všech procesů informačními systémy ve své působnosti,
- prosazuje opatření nutná pro zajištění bezpečnosti informací, v rámci své působnosti kontroluje plnění povinností a zajištění souladu s interní dokumentací,
- akceptuje rizika plynoucí z bezpečnostních výjimek (Příloha č. 6) ve své působnosti,

[2] *RA 02 Organizační řád*: Ředitelé sekcí, vedoucí odborů a vedoucí oddělení se označují jako vedoucí zaměstnanci společnosti ve smyslu Zákoníku práce.

- odpovídá za oddělení rolí a odpovědností mezi oblastmi provozu IS/ICT a bezpečnosti informací ve své působnosti.

Člen představenstva pověřený řízením úseku *Řízení společnosti a energetického majetku*:

- řídí oblasti ICT a vytváří dostatečné zdroje tak, aby ICT ČEPS byly rozvíjeny a obnovovány bezpečným způsobem a aby podporovaly plnění cílů společnosti s ohledem na existující rizika ve své působnosti,
- zajišťuje kontinuitu činností ICT a požadovanou podporu všech procesů ICT ve své působnosti,
- prosazuje opatření nutná pro zajištění bezpečnosti informací, v rámci své působnosti kontroluje plnění povinností a zajištění souladu s interní dokumentací,
- akceptuje rizika plynoucí z bezpečnostních výjimek (Příloha č. 6) ve své působnosti,
- odpovídá za oddělení rolí a odpovědností mezi oblastmi provozu ICT a bezpečnosti informací ve své působnosti.

Člen představenstva pověřený řízením úseku *Provoz a údržba*:

- řídí oblasti ICT a vytváří dostatečné zdroje tak, aby ICT ČEPS byly provozovány bezpečným způsobem a aby podporovaly plnění cílů společnosti s ohledem na existující rizika ve své působnosti,
- zajišťuje kontinuitu činností ICT a požadovanou podporu všech procesů ICT ve své působnosti,
- prosazuje opatření nutná pro zajištění bezpečnosti informací, v rámci své působnosti kontroluje plnění povinností a zajištění souladu s interní dokumentací,
- akceptuje rizika plynoucí z bezpečnostních výjimek (Příloha č. 6) ve své působnosti,
- odpovídá za oddělení rolí a odpovědností mezi oblastmi provozu ICT a bezpečnosti informací ve své působnosti.

Ředitelé sekcí *Energetické řídící a informační systémy, ICT služby* zajišťují provoz a rozvoj ICT v souladu s požadavky na bezpečnost informací ve své působnosti.

Ředitel sekce *Řízení provozu a údržby* zajišťuje provoz ICT ve své působnosti v souladu s požadavky na bezpečnost informací.

Ředitel sekce *Rozvoj a technická koncepce PS* zajišťuje rozvoj ICT ve své působnosti v souladu s požadavky na bezpečnost informací.

Ředitel sekce *Správa energetického majetku* zajišťuje obnovu ICT ve své působnosti v souladu s požadavky na bezpečnost informací.

Bezpečnostní ředitel odpovídá za výkon povinností ve všech oblastech bezpečnosti podle ustanovení RA 06.

Vedoucí oddělení *Strategie a bezpečnost ICT* plní roli manažera bezpečnosti informací (MBI). Povinnosti, odpovědnosti a rozsah oprávnění manažera bezpečnosti informací jsou podrobně vymezeny v Příloze č. 4.

Vedoucí útvaru (viz Příloha č. 11) - odpovídá za vypracování plánu kontinuity a činností útvaru.

Ředitel sekce *Podpůrné činnosti*:

- zavádí a provozuje opatření v oblasti fyzické bezpečnosti, požární ochrany a zajišťuje vhodné provozní prostředí pro informační systémy.

Vedoucí odboru *Personalistika:*

- specifikuje požadavky na bezpečnost informací před zahájením pracovního vztahu se zaměstnancem, v průběhu nebo změně pracovního vztahu a při jeho ukončení,
- zahrnuje požadavky na bezpečnost informací v katalogu pracovních funkcí,
- odpovídajícím způsobem prověřuje bezúhonnost, kvalifikaci a reference uchazečů o zaměstnání,
- odpovídá za seznámení nových zaměstnanců s touto směrnicí a s dalšími interními bezpečnostními dokumenty v rozsahu odpovídajícím jejich pracovním povinnostem,
- zajišťuje (ve spolupráci se specialisty oddělení Strategie a bezpečnost ICT) školení zaměstnanců o bezpečnosti informací,
- poskytuje informace pro zřízení odpovídajícího přístupu do IS pro nové zaměstnance,
- definuje postihy za nedodržení pravidel bezpečnosti informací,
- je oprávněn požadovat součinnost jiných útvarů při zavádění požadavků bezpečnosti informací do pracovních smluv.

Risk Manager:

- ve spolupráci s vedoucím odboru Strategie a R&D aktualizuje katalog strategických rizik[3] včetně způsobu jejich ošetření
- jednou ročně předkládá představenstvu Zprávu o řízení rizik
- povinnosti, odpovědnosti a rozsah oprávnění Risk Managera jsou vymezeny v SM/75 Řízení rizik ve společnosti ČEPS.

Právní služba se vyjadřuje v rozsahu své působnosti k souladu navrhovaných opatření či právních úkonů s obecně závaznými právními předpisy.

[3] Strategické riziko SR3 – Napadení kritické infrastruktury ČEPS a živelné pohromy

4 ŘÍZENÍ A ZVLÁDÁNÍ RIZIK BEZPEČNOSTI INFORMACÍ

Řízení bezpečnosti informací společnosti je založeno na řízení rizik bezpečnosti informací. Ve společnosti je stanovena metodika a přístup k jejich hodnocení (posouzení) a zvládání (ošetření). Metodiku včetně odpovědností, pravomocí a potřebné součinnosti stanovuje Příloha č. 12 SM/88.

5 MĚŘENÍ ÚČINNOSTI PROCESŮ BEZPEČNOSTI

Pro zajištění efektivního řízení a kontinuálního zlepšování systému řízení bezpečnosti informací společnost ČEPS provádí měření účinnosti procesů a opatření ISMS. Výstupy z měření jsou využity při stanovování priorit ISMS na další období.
Měření je založeno na kvalitativním vyhodnocení, zda procesy (dílčí činnosti) ISMS, požadované normou ISO/IEC 27001, probíhají, jak byly naplánovány. Měření spočívá v odpovědi na otázku typu: „Je v organizaci ustaven a používán daný proces tak, jak je specifikováno v normě ISO/IEC 27001?“
Měření se provádí alespoň jednou ročně. Za proces tohoto měření, včetně analýzy a vyhodnocení výsledků odpovídá manažer bezpečnosti informací.
Měření účinnosti opatření zkoumá kvantitativně, nakolik jsou naplněna opatření a doporučení vycházející z provedené analýzy rizik v prostředí webové aplikace RAMSES. Doporučená bezpečnostní opatření aplikace RAMSES jsou navázána na opatření přílohy A normy ISO/IEC 27001. Měření spočívá v hodnocení míry naplněnosti opatření přílohy A normy ISO/IEC 27001 implementací sady opatření z knihovny RAMSES. Hodnocení se provádí kontinuálně tak, jak se mění stav implementace opatření. Za proces tohoto měření, včetně analýzy a vyhodnocení výsledků, odpovídá manažer bezpečnosti informací.
Uvedené metriky budou průběžně přehodnocovány a aktualizovány z pohledu jejich účinnosti.

6 ORGANIZACE INFORMAČNÍ BEZPEČNOSTI

Všichni zaměstnanci se musí v rámci své působnosti podílet na ochraně aktiv společnosti. Působení útvarů společnosti při prosazování bezpečnosti musí být koordinované a soustavné.
Pokud je to možné, je nutno v organizační struktuře uplatňovat princip oddělení pravomocí. Každý zaměstnanec musí mít jen takové pravomoci a takové přístupy k informacím, jaké nezbytně potřebuje pro výkon svých pracovních povinností.

Organizace uvnitř společnosti

Role, odpovědnosti a pravomoci v oblasti informační bezpečnosti definuje kap. 3.2.

Vztahy s externími subjekty

Musí být v souladu s ustanoveními RA 06.
Před povolením přístupu k informacím a systémům společnosti musí být posouzena možná rizika.
Smluvní vztah s dodavatelem musí obsahovat požadavky na zajištění bezpečnosti informací formou:

- dohody nebo smlouvy o úrovni služeb (Service Level Agreement - SLA),
- dohody o zachování mlčenlivosti (Non Disclosure Agreement - NDA).

7 ŘÍZENÍ AKTIV A KLASIFIKACE INFORMACÍ

Bezpečnost všech informačních aktiv společnosti i aktiv informačních a komunikačních systémů musí být řízena a udržována způsobem odpovídajícím jejich významu a důležitosti pro společnost.

Odpovědnost za aktiva

Významná aktiva společnosti musí být evidována. Musí být určeni jejich vlastníci a stanovena odpovědnost vlastníků za udržování přiměřených bezpečnostních opatření. Odpovědnost za zajištění bezpečnosti aktiva nese jeho vlastník, odpovědnost za realizaci bezpečnostních opatření může být delegována.

Klasifikace informací

Informace zpracovávané a ukládané v IS ČEPS jsou rozdílné hodnoty a mají pro společnost různý význam. Klasifikací musí být určena jejich potřebnost, důležitost, stupeň ochrany i způsob zacházení s nimi. Klasifikace informací a manipulační postupy podle klasifikačních stupňů jsou upraveny Přílohou č. 1.

V ČEPS je použito schéma:

KLASIFIKAČNÍ SCHÉMA	
Klasifikační stupeň	**Popis**
CITLIVÉ INTERNÍ (C_INT)	Informace, jejichž vyzrazení by mohlo **závažným způsobem poškodit** fungování a dobré jméno ČEPS, způsobit závažné finanční ztráty nebo ohrozit stabilitu přenosové soustavy.
INTERNÍ (INT)	Většina běžně provozně užívaných informací ČEPS pro interní potřebu a výkon pracovních povinností. Tyto informace jsou **citlivé z pohledu zveřejnění mimo společnost.**
VEŘEJNÉ (PUB)	Informace, které jsou určeny ke zveřejnění.

8 BEZPEČNOST LIDSKÝCH ZDROJŮ

Bezpečnost v pracovním vztahu

Řízení bezpečnosti v pracovním vztahu spadá do kompetence odboru Personalistika.
Bezpečnost informací musí být řízena po celou dobu pracovního vztahu[4] zaměstnance. Odpovědnost za bezpečnost informací musí být zohledněna v rámci přijímacího řízení, musí být zahrnuta v pracovní smlouvě a v katalogu pracovních funkcí. Zaměstnanci přicházející při plnění pracovních povinností do styku s informacemi klasifikovanými stupněm INTERNÍ nebo CITLIVÉ INTERNÍ musí před přidělením přístupu k těmto informacím podepsat prohlášení o mlčenlivosti.
Při ukončování pracovního vztahu zaměstnance musí jeho vedoucí zajistit vrácení všech informačních aktiv nebo jejich převedení na jiného zaměstnance. Vedoucí odcházejícího, propouštěného nebo přeřazovaného zaměstnance požaduje a kontroluje odebrání (změnu) jeho přístupových práv k informačním systémům a informacím.

[4] Zaměstnání (pracovní poměr na dobu určitou nebo neurčitou), přidělení pracovní role, změna pracovní role, dohoda o pracovní činnosti, dohoda o provedení práce anebo ukončení jakékoli z těchto vazeb

Bezpečnostní povědomí, vzdělávání a školení v oblasti bezpečnosti informací

Zaměstnanci a externí subjekty musí být seznámeni se svými povinnostmi v oblasti bezpečnosti informací tak, aby bylo sníženo riziko chyby, krádeže, podvodu nebo jiného zneužití informačních aktiv společnosti.

Zaměstnanci společnosti musí:

- být před udělením přístupu do IS seznámeni s touto směrnicí a s navazujícími dokumenty informační bezpečnosti v rozsahu odpovídajícím jejich pracovním povinnostem,
- absolvovat pravidelně minimálně 1 x za rok se opakující školení v oblasti bezpečnosti informací,
- znát postupy hlášení bezpečnostních událostí, slabin, chyb a incidentů, které mohou mít dopad na bezpečnost společnosti.

Zaměstnanci externího subjektu musí:

- být před udělením přístupu do IS seznámeni s touto směrnicí a s bezpečnostními pravidly a zásadami týkajícími se obsahu jejich práce (Příloha č. 3), toto seznámení zajišťuje zaměstnanec s odpovědností za smluvní vztah s externím subjektem,
- znát postupy hlášení bezpečnostních událostí, slabin, chyb a incidentů, které mohou mít dopad na bezpečnost společnosti.

9 FYZICKÁ BEZPEČNOST A BEZPEČNOST PROSTŘEDÍ

Fyzická bezpečnost informačních aktiv, prostorů a provozního prostředí musí odpovídat zjištěným bezpečnostním rizikům a musí být v souladu s ustanoveními Přílohy č. 1 a směrnice SM/85. Manažer bezpečnosti informací a ředitelé sekcí *Energetické řídící a informační systémy, ICT služby a Řízení provozu a údržby* navrhují sekci *Podpůrné činnosti* opatření fyzické bezpečnosti v oblasti ICT na základě výsledků analýzy rizik a v souladu s dalšími vnitřními předpisy.

Chráněné prostory

Zařízení pro zpracování informací společnosti (servery, datová úložiště, síťové prvky apod.) musí být umístěna ve *zvláště chráněných prostorech* chráněných prostředky fyzické ochrany a režimovými opatřeními; stojany (racky), ve kterých jsou tato zařízení umístěna, musí zůstávat uzamčeny.

Bezpečnost zařízení

Zařízení určená pro práci s informacemi společnosti (pracovní stanice, notebooky, servery, disková úložiště, prvky síťové infrastruktury apod.) musí být fyzicky chráněna proti bezpečnostním hrozbám a působení vnějších vlivů. Ochrana zařízení společnosti (včetně těch, která se používají mimo prostory společnosti) musí být zajištěna proti:

- neautorizovanému přístupu k datům,
- ztrátě,
- poškození zařízení ze strany potenciálních útočníků nebo přírodních hrozeb (požár, voda, přírodní katastrofa atd.).

Zařízení musí být provozována v souladu s provozními podmínkami výrobce a chráněna proti výpadkům nebo anomáliím napájení. Kabelové komunikační rozvody musí být chráněny před odposlechem nebo poškozením. Zařízení obsahující paměťová média musí být před svým vyřazením nebo změnou použití bezpečně vymazána, případně zlikvidována bez dalšího využití (sešrotována).

10 ŘÍZENÍ PROVOZU IS/ICT

Provozní postupy a odpovědnosti

Zajištěn musí být správný a bezpečný provoz všech prostředků pro zpracování informací ČEPS, které jsou buď přímo ve správě společnosti, nebo ve správě externích subjektů. Odpovědnosti za zajištění bezpečnosti informací jsou uvedeny v kap. 3.2.
Uplatňováno musí být oddělení povinností a odpovědností tak, aby bylo sníženo riziko úmyslného zneužití systému nebo riziko chyb z nedbalosti.
Dodržována musí být zásada oddělení vývojového prostředí od provozního.
Provozní postupy pro správu informačních systémů musí být dokumentovány v rozsahu zálohování, řízení HelpDesku, přidělování přístupů, řízení kapacit, schvalování systému do provozu, řízení změn v informačním systému a postupů obnovy po havárii.
Tam, kde není možné oddělení povinností a odpovědností a oddělení vývojového prostředí od provozního, musí být provozní postupy řešeny udělením výjimky (Příloha 6 SM/88).

Řízení dodávek a služeb

U každé dodávky služby nebo produktu v oblasti ICT musí být zvážena bezpečnostní rizika. Rizika s možným dopadem na bezpečnosti informací musí být konzultována se specialisty bezpečnosti informací, kteří jsou oprávněni kontrolovat dodržování a zajištění dohodnutých bezpečnostních parametrů. Změny dodávek a služeb musí být součástí procesu řízení změn v ICT. Zvláštní péči je nutno věnovat výběru pracovníků, smluvnímu zajištění a důsledné kontrole služeb externích subjektů (kap. 6).

Správa IS/ICT

Při provozu a rozvoji informačních systémů musí být:

- řízena správa zařízení a sítí včetně vývoje a implementace nových systémů a řízení jejich změn,
- udržována dokumentace o aktivech IS, prostředí IS a síťové infrastruktury i konfiguraci významných komponent ICT (konfigurační standardy serverů, datových úložišť, síťových prvků, koncových stanic apod.),
- zajišťována bezpečnosti informací v procesu řízení změn v ICT,
- schvalována manažerem bezpečnosti informací v rámci procesu řízení změn v ICT každá změna prostředí ICT s dopadem na informační bezpečnost,
- zajišťována bezpečnost v počítačových sítích, zejména jsou-li pro komunikaci využity veřejné sítě,
- vytvářeny a jedenkrát ročně testovány plány pro obnovu hlavních informačních systémů po havárii (kap. 14).

Manažer bezpečnosti informací stanovuje požadavky na dodržení zásad bezpečnosti informací v souladu s řídícími dokumenty a schvaluje realizaci bezpečnostních opatření pro ochranu informací.

Ochrana proti škodlivým programům

Zavedena musí být opatření pro prevenci a detekci škodlivých programů a definovány postupy pro zotavení po útoku.
Součástí ochrany musí být zvyšování povědomí o bezpečnostních hrozbách mezi zaměstnanci.

Monitorování

Informační systémy společnosti musí být monitorovány a musí být zaznamenávány události s možným dopadem na bezpečnost s cílem detekovat a předcházet bezpečnostním incidentům.
Informační systémy určené opatřením obecné povahy NBÚ (ZKB) a další významné informační systémy společnosti musí předávat auditní záznamy v reálném čase do centrálního systému pro vyhodnocování bezpečnostních událostí (SIEM)
Záznamy (logy) musí být uchovávány po definovanou dobu tak, aby bylo zabráněno neoprávněnému přístupu k nim a jejich falšování, v případě systémů napojených do SIEM systému je toto zajištěno vlastnostmi SIEM systému. Za události s možným dopadem na bezpečnost jsou považovány i záznamy o chybách a selháních IS.

Řízení zranitelností

Ve společnosti musí být zaveden proces řízení zranitelností ICT, který zajistí včasné získání informací o technických zranitelnostech v provozovaných informačních systémech, jejich vyhodnocení a odstranění (Příloha č. 7).

11 ŘÍZENÍ PŘÍSTUPU

Přístup k informačním aktivům společnosti musí být řízen v souladu s bezpečnostními požadavky (Příloha č. 5). Přístup bez povolení je zakázán a je považován za porušení povinnosti zaměstnance vyplývající z právních a interních předpisů vztahujících se k zaměstnancem vykonávané práci zvlášť hrubým způsobem.

12 POŘÍZENÍ, VÝVOJ A ÚDRŽBA INFORMAČNÍCH SYSTÉMŮ

Při pořízení, vývoji a údržbě IS musí být dodržovány zásady bezpečnosti informací:

- u nově pořizovaných informačních systémů musí být požadavky bezpečnosti specifikovány již v zadání na nákup nebo vývoj systému,
- v IS musí být přijata opatření na zajištění kontroly vstupních informací, správnosti zpracování a kontroly výstupních informací,
- v případě zvýšených požadavků na zajištění důvěrnosti a integrity informací musí být využita kryptografická opatření,
- přístup ke knihovnám zdrojových kódů musí být řízen a zdrojové kódy nesmí být dostupné z provozního prostředí IS,
- správa, vývoj a implementace nových IS musí podléhat procesům řízení změn v ICT a musí být v souladu s kap. 10 a navazujícími vnitřními předpisy,
- zpracování ročních plánů preventivní údržby systémů a zařízení je v kompetenci ředitelů příslušných sekcí ICT,
- významné nově implementované systémy musí mít auditní funkcionality a musí být zapojeny do systému pro centrální sběr bezpečnostních událostí (SIEM).

13 ŘÍZENÍ BEZPEČNOSTNÍCH INCIDENTŮ

Ve společnosti musí být zaveden proces řízení incidentů bezpečnosti informací. Proces musí zajistit nahlášení bezpečnostních událostí, slabin a jiných bezpečnostních incidentů v IS způsobem, který umožní včasné zahájení kroků vedoucích k nápravě (Příloha č. 8).

Bezpečnostní události jsou identifikovány pomocí automatického systému pro sběr a vyhodnocování bezpečnostních událostí (SIEM) i prostřednictvím hlášení uživatelů.
Všichni zaměstnanci ČEPS i externích subjektů přistupující do infrastruktury společnosti jsou povinni znát postupy hlášení bezpečnostních událostí (kap. 8).

14 ŘÍZENÍ KONTINUITY ČINNOSTÍ IS/ICT

Zajištění kontinuity činností IS/ICT a trvalé podpory procesů informačními systémy je součástí řízení společnosti. Cílem je minimalizovat negativní dopady mimořádných událostí a bezpečnostních incidentů na procesy společnosti a zajistit rychlé zotavení ze ztráty informačních aktiv. Řízení kontinuity činností IS/ICT předpokládá vytvoření havarijních plánů a plánů obnovy funkčnosti všech důležitých systémů společnosti. Havarijní plány a plány obnovy musí být zpracovány, pravidelně aktualizovány a testovány v souladu s Přílohou č. 10.

Řízení kontinuity IS/ICT musí zajistit:

- identifikaci kritických činností společnosti,
- ohodnocení následků závažných bezpečnostních incidentů (přírodních pohrom, bezpečnostních narušení nebo ztráty dostupnosti služeb),
- vytvoření opatření k identifikaci a minimalizaci rizik,
- vytvoření opatření pro omezení následků incidentů,
- včasnou dostupnost informací potřebných pro obnovení klíčových činností společnosti.

15 SOULAD S POŽADAVKY

Soulad s požadavky legislativy

Návrh, provoz a používání informačních systémů musí být v souladu s obecně závaznými právními předpisy.

Soulad s interními pravidly

Soulad stavu informační bezpečnosti s bezpečnostními pravidly a zásadami definovanými touto směrnicí a navazujícími dokumenty musí být pravidelně přezkoumáván. Provádí se formou auditu, bezpečnostními analýzami, analýzami rizik, penetračními testy apod.

16 PŘECHODNÁ A ZRUŠOVACÍ USTANOVENÍ, ÚČINNOST

Přechodná ustanovení nejsou.

Ruší se 9. znění směrnice SM/88/2016.

Toto 10. znění směrnice SM/88/2016 nabývá účinnosti dne 11. 10. 2016.

17 SEZNAM SAMOSTATNÝCH PŘÍLOH

Příloha č. 1 *Klasifikace a ochrana informací a práce s nimi (V-5)*
Příloha č. 2 *Pravidla informační bezpečnosti pro uživatele IS (V-5)*
Příloha č. 3 *Pravidla informační bezpečnosti pro provozovatele a administrátora IS (V-6)*
Příloha č. 4 *Pravidla práce manažera bezpečnosti informací (V-5)*
Příloha č. 5 *Řízení přístupu (V-6)*
Příloha č. 6 *Řízení výjimek informační bezpečnosti (V-6)*
Příloha č. 7 *Řízení zranitelností ICT (V-6)*
Příloha č. 8 *Řízení bezpečnostních incidentů (V-5)*

Příloha č. 9 *Práce s datovými médii (V-6)*
Příloha č. 10 *Zásady pro vytvoření plánů kontinuity a obnovy ICT (V-4)*
Příloha č. 11 *Doporučené zásady pro vytvoření plánů kontinuity a obnovy činností útvaru (V-3)*
Příloha č. 12 *Řízení rizik bezpečnosti informací (V-1)*