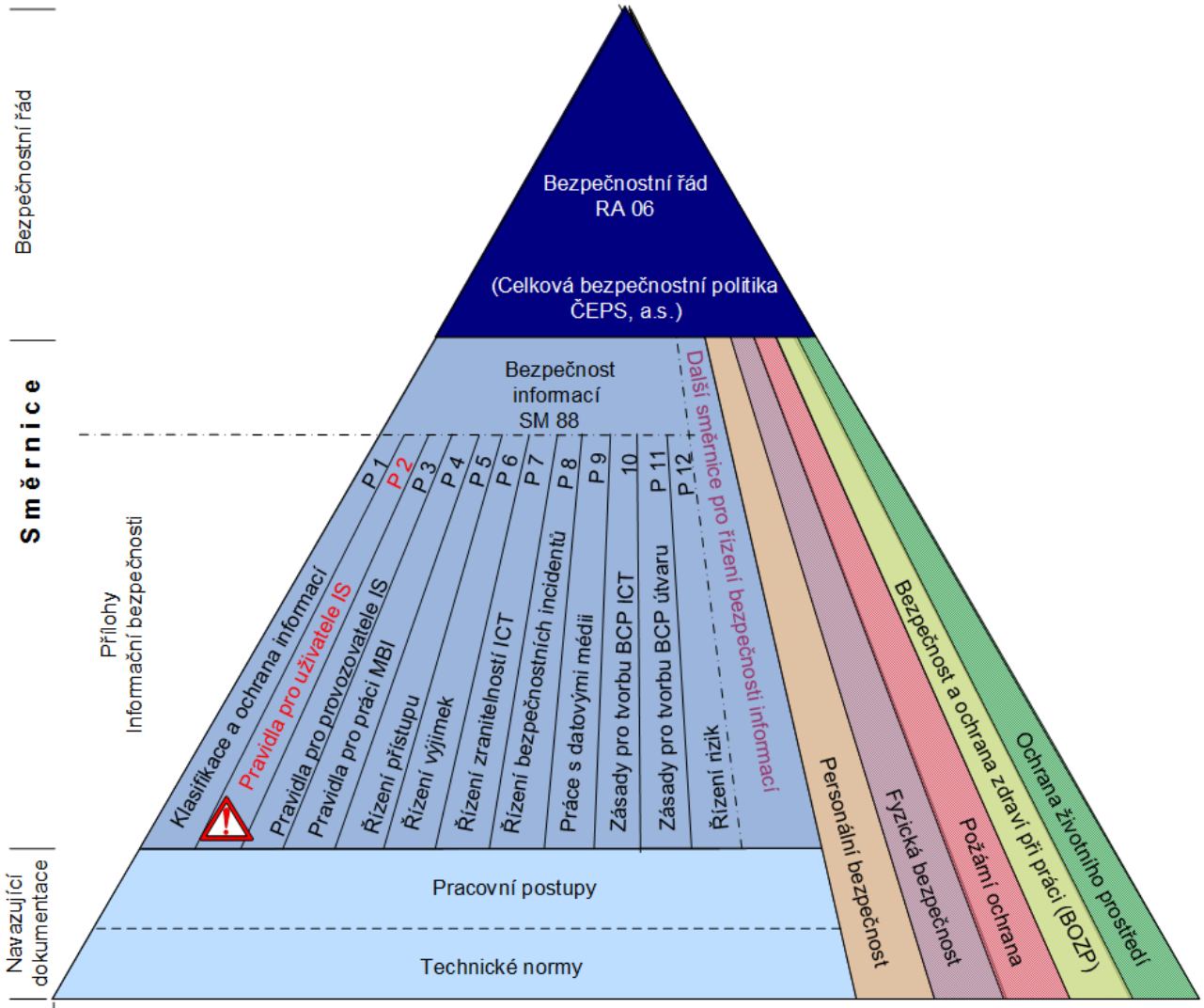
PRAVIDLA BEZPEČNOSTI INFORMACÍ PRO UŽIVATELE IS

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, PŮSOBNOST A ODPOVĚDNOST

Dokument *Pravidla bezpečnosti informací pro uživatele IS* je samostatnou přílohou směrnice *Bezpečnost informací* (dále „SM/88“), která stanovuje základní principy, pravidla a požadavky bezpečnosti informací. Tato příloha určuje pravidla, která zavazují uživatele IS k dodržování standardů chování při práci s informačním systémem ČEPS, a.s. (dále „ČEPS“ nebo „společnost“) tak, aby byla zajištěna bezpečnost informací.

Příloha se vztahuje na práci s informacemi a informačními systémy v působnosti všech procesů a činností ve společnosti a je závazná pro všechny zaměstnance ČEPS a spolupracující externí subjekty.

1.1 Role, odpovědnosti a pravomoci

Zaměstnanci jsou uživateli informací a informačních systémů ČEPS. Jejich základní odpovědnosti a pravomoci jsou uvedeny v SM/88. Pravidla pro práci s informacemi stanovuje její Příloha č. 1. Pravidla chování uživatelů v prostředí ICT, odpovědnosti a pravomoci zaměstnanců v oblasti informační bezpečnosti určuje tato Příloha č. 2.

Seznámení zaměstnanců společnosti s tímto dokumentem provádí odbor Personalistika, externí subjekty musí být k dodržování vázány smluvně.

Vedoucí zaměstnanci v rámci své působnosti kontrolují seznámení zaměstnanců s těmito pravidly i s ostatní bezpečnostní dokumentací a sledují jejich dodržování.

Manažer bezpečnosti informací (MBI) odpovídá (ve vztahu k tomuto dokumentu) za:

- jeho pravidelnou revizi
- udělování výjimek v souladu s Přílohou č. 6 SM/88.

Povinnosti a pravomoci manažera bezpečnosti informací jsou definovány v Příloze č. 4 SM/88.

2 KLASIFIKACE INFORMACÍ

Klasifikaci informací provádí jejich vlastník v souladu s Přílohou č. 1 SM/88 a uživatelé jsou povinni se při práci s informacemi řídit pravidly danými tímto dokumentem.

3 INFORMAČNÍ SYSTÉMY A INFORMAČNÍ TECHNOLOGIE

3.1 Přihlašování a používání hesel

Pro běžný přístup do IS ČEPS uživatel používá uživatelské jméno (účet) a heslo. Ve vybraných případech se používá dvoufaktorová autentizace (uživatelské jméno a heslo ve spojení s autentizačním předmětem, pinem). Při výběru a používání hesel musí uživatelé dodržovat stanovené bezpečnostní postupy a pravidla.

Uživatelé jsou povinni:

- přistupovat do systému pouze prostřednictvím **svého** uživatelského účtu a hesla
- držet hesla v tajnosti
  - hesla nesmí být jakýmkoliv způsobem sdílena s jinými uživateli
  - hesla nesmí být zaznamenána na papíře, v souborech nebo na přenosných zařízeních v nešifrované podobě
  - při kompromitaci nebo podezření na kompromitaci musí být hesla ihned změněna
- dodržovat požadavky na strukturu hesla

  - délka je minimálně 8 znaků v kombinaci alfanumerických (malá, velká písmena), numerických a zvláštních znaků
  - jsou zapamatovatelná
  - neobsahují informace vztahující se k uživateli (jména blízkých osob, telefonní čísla, datum narození, atd.) nebo po sobě jdoucí stejné znaky
  - neskládají se pouze z čísel či písmen nebo ze slov vyskytujících se ve slovnících
- na výzvu systému měnit hesla a neopakovat žádné z pěti posledních použitých hesel
- změnit bez prodlení dočasná hesla při prvním přihlášení
- nikdy neukládat hesla do automatizovaného přihlašovacího procesu (např. do internetového prohlížeče, maker nebo funkčních kláves)
- zajistit bezpečnost autentizačních předmětů.

Uživatelský účet:

- může být zablokován na žádost manažera bezpečnosti informací při vážném porušení pravidel bezpečnosti informací
- je zrušen nebo blokován, dojde-li k ukončení pracovního poměru nebo k převedení pracovníka do jiného útvaru
- je zrušen nebo blokován, není-li používán déle, než tři měsíce
- je zablokován po 50-ti neúspěšných pokusech o přihlášení; v tomto případě musí uživatel vyčkat 5 minut nebo prostřednictvím kontaktního místa HelpDesku ICT požádat o odblokování účtu.

Hesla a další autentizační údaje jsou CITLIVÉ INTERNÍ informace a jejich vyzrazení je považováno za bezpečnostní incident. Uživatel ho musí hlásit v souladu s postupem v kap. 4.

Uživatel je odpovědný za veškeré akce prováděné z jeho účtu a nesmí umožnit práci pod svým účtem jiné osobě.

3.2 Řízení přístupu k informačním systémům

Přístupová oprávnění k IS jsou uživatelům přiřazována na základě pracovního zařazení. V případě, že uživatel má vedoucím zaměstnancem pro výkon svých pracovních povinností schválena další oprávnění, žádá o ně prostřednictvím HelpDesku ICT.

Uživatelé jsou povinni řídit se nastavenými pravidly řízení přístupu a nesmějí tato pravidla měnit ani obcházet.

Externí subjekty mohou získat oprávnění přístupu nutná pro výkon jejich služby na základě smluvního ujednání vždy pouze na dobu určitou. Řízení přístupu uživatelů je realizováno v souladu s Přílohou č. 5 SM/88.

3.3 Uživatelská zařízení ICT

Uživatel smí používat pouze zařízení ICT, které mu bylo společností svěřeno nebo zařízení k tomuto účelu nebo použití schválené, a to v rozsahu nezbytném pro výkon svých pracovních povinností. Při užívání těchto zařízení musí dodržovat základní povinnosti zaměstnanců dle ustanovení RA 07 a ustanovení SM/96. Používání jiných zařízení a jejich připojování do IS ČEPS je nepřípustné. Uživatelé nesmí zpracovávat a uchovávat informace společnosti na nepovolených zařízeních, jako např. soukromé počítače, tablety, veřejné servery apod. Uživatelé mají na svěřeném zařízení pouze základní oprávnění USER. Výjimky lze udělit pouze v odůvodněných případech a na dobu nezbytně nutnou. Technologické notebooky, u kterých používaná aplikace vyžaduje trvalé nastavení oprávnění LOCAL ADMINISTRATOR, nesmí být připojovány do sítě ČEPS.

Uživatel nesmí měnit hardwarovou ani softwarovou konfiguraci zařízení ICT, ani jeho základní nastavení. V případě, že je nutná pro jeho práci změna konfigurace, kontaktuje HelpDesk ICT.

Má-li uživatel v odůvodněné výjimce na své pracovní stanici či notebooku nastavena administrátorská oprávnění, nesmí měnit standardní bezpečnostní nastavení, zejména:

- vypínat bezpečnostní mechanizmy např. osobní firewall nebo antivirový program
- nastavovat dlouhodobé sdílení disků nebo tiskáren
- rušit šifrování disku
- mazat uložené certifikáty
- měnit nebo nastavovat jiná než schválená vzdálená připojení (VPN)
- používat prostředky pro identifikaci přístupových hesel.

Uživatelé notebooků jsou povinni:

- připojit notebook nejdéle po 14-ti dnech do LAN ČEPS (ne přes VPN) a vyčkat provedení všech automatických servisních úkonů. Výjimku mají uživatelé, kteří prokazatelně ze zdravotních či pracovních důvodů (dovolená, služební cesta) nemohou tento požadavek splnit. V tomto případě musí uživatel, před opětovným zapojením přístroje do sítě LAN, nechat jej zkontrolovat pracovníky odboru Řízení kontraktů IT a Helpdesk, sekce ICT služby.
- používat notebook na veřejných místech tak, aby byla minimalizována rizika
  - odcizení a poškození (neponechávat notebook bez dozoru na nechráněných místech, např. zavazadlový prostor dopravního prostředku)
  - odposlechu komunikace
  - odpozorování informací neautorizovaným způsobem
- zachovávat důvěrnost uložených informací předepsaným způsobem (šifrování dat)
- pro vzdálený přístup do sítě ČEPS používat pouze schválené komunikační technologie (VPN)

Uživatelé chytrých telefonů a tabletů jsou povinni:

- umožnit zařazení telefonu a tabletu do centrální správy mobilních zařízení (MDM)[1]
- chránit mobilní zařízení
  - heslem (PINem, bezpečnostním znakem, otiskem prstu) a antivirovým softwarem
  - aktivací funkce automatického uzamční zařízení max. po 15 vteřinách nečinnosti
- dbát na fyzickou bezpečnost firemního mobilního zařízení, svěřené zařízení nesmí zůstat ponecháno bez dozoru, zejména pak ve veřejných prostorách, pokud je nutné zařízení odložit (např. při sportovních aktivitách), musí být uloženo na bezpečném místě tak, aby nebylo zbytečně na očích
- v případě ztráty nebo krádeže mobilního zařízení událost neprodleně nahlásit na určené kontaktní místo (viz kap. 6) a postupovat v souladu se směrnicí SM/72 *Nákup, evidence a používání mobilních telefonů v ČEPS, a.s.*
- pokud není datové úložiště v mobilním zařízení šifrováno, neuchovávat v něm INTERNÍ firemní informace
- vypnout nebo zablokovat vlastnosti a aplikace, které nejsou na mobilních zařízeních používány (např. Bluetooth, wi-fi, určování polohy)
- používat pouze oficiální zdroje aplikací a důsledně kontrolovat jejich práva
- nepůjčovat zařízení jiným osobám.

Nástrojem pro centrální správu mobilních zařízení lze mj. zajistit:

[1] Bude upřesněno v Příloze 18 SM/104 *Pravidla pro užití mobilních zařízení v ČEPS.*

- zabezpečení heslem (PINem, bezpečnostním znakem, otiskem prstu) a antivirovým softwarem
- bezpečné smazání všech firemních dat v případě, že je zařízení předáváno k servisnímu zákroku
- bezpečné smazání všech dat v případě ztráty zařízení nebo odchodu zaměstnance ze společnosti.

3.4 Neobsluhovaná uživatelská zařízení

Uživatelé jsou při přerušení nebo ukončení práce se zařízením ICT povinni:

- ukončit aktivní relace, uzamknout pracovní stanici nebo jinak zajistit, že zařízení nebude otevřené k neautorizovanému přístupu při krátkodobém přerušení práce (klávesovou kombinací Windows klávesa + L, nebo klávesovou trojkombinací CTRL+ALT+DEL s následující volbou "Uzamknout stanici")
- zařízení vypnout při ukončení práce, pokud jej provozovatel IS nevyzve jinak
- fyzicky zajistit mobilní výpočetní a paměťová zařízení (notebooky, telefony, PDA, USB a flash disky atp.).

Po 15-ti minutové nečinnosti je uzamčení pracovní stanice vyvoláno automaticky doménovou politikou.

3.5 Zásada prázdného stolu a prázdné obrazovky monitoru

Uživatelé jsou povinni zamezit možnosti neoprávněného přístupu k informacím společnosti, jejich ztrátě či poškození, a proto musí:

- fyzicky zabezpečit klasifikované informace (papírové dokumenty a počítačová média) dle pravidel Přílohy č. 1 SM/88 v případě, že se právě nepoužívají
- pro síťové tisky využívat pouze tisk s řízeným přístupem (tiskne se až po autentizaci uživatele na tiskárně)
- ihned po vytištění odebrat dokumenty z tiskárny, zejména pokud jde o síťovou tiskárnu umístěnou ve společných prostorech
- nenechávat zdrojové dokumenty v kopírovacích strojích, skenerech nebo jiných vstupních zařízeních
- dodržovat pravidla kap. 3.4.

3.6 Ochrana proti škodlivým programům

Uživatelé jsou povinni spolupracovat se správci IS na ochraně informačních systémů společnosti před zavlečením škodlivých programů (viry, červy, trojské koně apod.), proto na svěřených zařízeních mají zakázáno:

- provozovat jiné než schválené programové vybavení
- modifikovat nastavení operačního systému, webového prohlížeče a jiných programů
- vypínat antivirovou ochranu
- zasahovat do běhu antivirových programů a jiné instalované ochrany
- vykonávat činnosti, při kterých se zvyšuje nebezpečí stažení škodlivých programů
  - vědomě navštěvovat neznámé webové stránky, ze kterých může hrozit zavlečení škodlivému programu
  - stahovat a přenášet na zařízení soubory neznámého původu
  - otevírat neznámé přílohy v e-mailech
  - používat jiné než povolené způsoby komunikace s externími subjekty.

3.7 Autorskoprávní ochrana a trestněprávní odpovědnost zaměstnanců

Zaměstnanci mají zakázáno stahovat a ukládat na lokální nebo sítová úložiště multimediální soubory, které nesouvisí s výkonem jejich práce pro zaměstnavatele, či s nimi jinak nakládat. Zákaz se týká především stahování, uchovávání či jiného nakládání s hudbou, filmy a počítačovými hrami. Takové bezlicenční nakládání s těmito multimédii na zařízeních zaměstnavatele je v rozporu s autorským zákonem (zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů). Konkrétně tímto jednáním může zaměstnanec spáchat přestupek podle autorského zákona anebo se může jednat i o správní delikt zaměstnavatele. V případě nikoli nepatrného zásahu do autorských práv třetích osob může zaměstnanec tímto jednáním spáchat dokonce trestný čin porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, postihovaný trestem odnětí svobody až 2 roky s tím, že je možné zároveň uložit pachateli peněžitý trest. Obdobně může být vedle pachatele podle zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, v platném znění, postižen za uvedený trestný čin i zaměstnavatel. Tím může zaměstnavateli vzniknout škoda, kterou bude zaměstnanec v takovém případě povinen nahradit. V podrobnostech jsou trestněprávní dopady jednání zaměstnance na zaměstnavatele blíže specifikovány v interním předpisu *RA 08 Trestněprávní program.*

Bez ohledu na shora uvedené veřejnoprávní sankce má za zákonem nepovolené nakládání s multimediálními soubory autor další práva, mimo jiné se domáhat náhrady vzniklé škody i přiměřeného zadostiučinění, a to i soudní cestou. Pokud zaměstnavateli v důsledku takového nelegálního jednání zaměstnance vznikne škoda způsobená úmyslně, hradí takový zaměstnanec v souladu se zákoníkem práce takto vzniklou škodu v plném rozsahu.

3.8 Zálohování a ukládání informací

Pravidelné zálohování dat uložených v informačních systémech společnosti je prováděno sekcemi Energetické a řídící informační systémy a ICT služby. Uživatel je povinen uchovávat všechna důležitá data na síťových úložištích (diskových polích a discích serverů). O případnou obnovu dat z těchto zdrojů uživatel může požádat prostřednictvím HelpDesku ICT.

Za data společnosti uložená na lokálních discích koncových stanic a notebooků odpovídá uživatel. Sekce ICT služby není schopna garantovat jejich obnovu.

Uživatel odpovídá za pravidelné synchronizování dat uložených na noteboocích s daty na síťových úložištích.

Pokud uživatelé ukládají data nebo provádějí individuální zálohy na média (DVD, flash disky, papír apod.), jsou povinni označovat, ukládat, likvidovat a jinak pracovat s médii v souladu s Přílohou č.1 SM/88.

3.9 Předávání informací

Uživatelé jsou povinni bez ohledu na způsob, médium nebo technologii dodržovat pravidla a postupy pro předávání nebo výměnu informací v souladu s Přílohou č. 1 SM/88.

Uživatelé mohou pro předávání a výměnu informací používat pouze schválené elektronické služby a prostředky.

Uživatelé nesmí zejména používat pro výměnu vnitropodnikových informací veřejné systémy, jako např.:

- Instant Messaging (IM), např. ICQ, Miranda, SIM, Yahoo, Jabber, apod.
- soukromé e-mailové schránky a freemailové služby, např. seznam, centrum, volny, gmail apod.
- webové diskusní skupiny, např. diskuse pod zpravodajskými články
- veřejné blogy
- sociální sítě.

3.10 **Pravidla užívání elektronické pošty**

Uživatel si při používání elektronické pošty musí být vědom, že prochází veřejným prostředím Internetu (zprávy mohou být odposlechnuty a přečteny jinými osobami než příjemcem, modifikovány, nemusí být doručeny včas nebo vůbec, mohou dorazit jinému příjemci než původnímu adresátovi).

Uživatelé jsou při používání elektronické pošty povinni:

- dbát pravidel klasifikace informací dle Přílohy č. 1 SM/88 a v souladu s ní používat schválené postupy a šifrovací prostředky pro zasílání příloh e-mailů
- vyplňovat položky "předmět" (subject) textem odpovídajícím obsahu a účelu zprávy; v textu zprávy je doporučeno informovat příjemce o tom, že odesíláme e-mail s přílohou (umožňuje to detekovat nevyžádané přílohy s možnou virovou nákazou)
- dodržovat kulturu a etiku e-mailové korespondence.

Uživatelé mají při používání elektronické pošty zakázáno:

- zneužívat elektronickou poštu pro zasílání nevyžádaných zpráv v rámci společnosti i vně
- zasílat e-mailové zprávy, které obsahují pomluvy, poplašné zprávy, hanlivé a vulgární výrazy nebo jinak uráží či snižují lidskou důstojnost
- otevírat nevyžádané, neznámé a potenciálně nebezpečné přílohy
- přihlašovat svou e-mailovou adresu do elektronických konferencí, pokud toto přímo nesouvisí s jejich pracovní náplní
- odpovídat na nevyžádanou poštu
- přesměrovávat firemní elektronickou poštu na jinou neschválenou elektronickou poštu
- užívat elektronickou poštu k soukromým účelům

3.11 **Pravidla užívání Internetu**

Internet je nástrojem pro komunikaci, získávání i předávání informací. Uživatel musí při užívání Internetu dodržovat SM/88, Přílohu P1 *Klasifikace a ochrana informací a práce s nimi* a následující pravidla:

- pracovní stanice se smí připojovat k Internetu prostřednictvím lokální sítě ČEPS
- pracovní stanice umístěné mimo objekty ČEPS (např. notebooky), pokud nepotřebují přistupovat k interním informacím společnosti, se smí připojovat k Internetu pomocí aplikace „Internet Proxy přepínač“
- uživatel Internetu musí dodržovat etická pravidla a musí mít na paměti, že přístup na Internet provádí také jménem společnosti (netiketa)
- poskytování CITLIVÝCH INTERNÍCH a INTERNÍCH informací prostřednictvím Internetu je zakázáno; Internet (veřejná síť) může být odposloucháván a poskytnuté informace nemusí být doručeny pouze na uživatelem určené místo
- přístup na Internet nesmí být zneužit k protiprávním účelům, jakými jsou např. nepovolený přístup do jiných informačních systémů na Internetu a získávání informací z nich

- přístup na Internet nesmí být využíván k soukromým účelům.

3.12 Monitorování provozu a činností

Pro ochranu informačních systémů, odhalování potenciálních útoků a bezpečnostních incidentů a pro vyhodnocování efektivity využití pracovních prostředků zaměstnanci je provoz informačních systémů monitorován.

V rámci monitoringu jsou zaznamenávány definované činnosti uživatelů, využití programového vybavení a je vyhodnocováno držení multimédií a her. Obsah zpráv elektronické pošty monitorován není, provádí se filtrace nevyžádané pošty (SPAM, SPYWARE, detekce virové nákazy apod.). Je zaznamenáván průběh zpracování mailů poštovními servery (odesílatel, příjemce, předmět, datum a velikost). U provozu internetu je monitorován objem uživatelem přenášených dat, navštívené webové stránky apod.

Provádí se automatizovaná analýza šifrované komunikace. Vyhodnocený nebezpečný provoz je systémem automaticky zablokován a data odstraněna.

4 HLÁŠENÍ A ŠETŘENÍ BEZPEČNOSTNÍCH INCIDENTŮ, ZRANITELNÝCH MÍST A CHYB

Uživatelé jsou povinni používat výpočetní systémy tak, aby svým jednáním předcházeli vzniku bezpečnostních incidentů nebo zranitelných míst v bezpečnosti ČEPS.

Jakoukoliv bezpečnostní událost či incident nebo podezření na něj, zranitelné místo nebo chybu v IS ČEPS, jsou uživatelé povinni oznámit na kontaktní místo (kap. 6).

Proces zvládání bezpečnostních incidentů podrobně popisuje samostatná Příloha č. 8 SM/88.

5 SOULAD S POŽADAVKY

Uživatelé jsou povinni dodržovat obecně závazné právní předpisy a pravidla i bezpečnostní opatření stanovená interní bezpečnostní dokumentací.

Veškerá ustanovení bezpečnostní dokumentace a jejich dodržování mohou být kontrolována.

Uživatelé jsou povinni aktivně spolupracovat při provádění bezpečnostních auditů a analýz, šetření bezpečnostních incidentů, a musí na vyžádání odpovědným pracovníků poskytnout informace potřebné pro hodnocení rizik.

6 KONTAKTNÍ MÍSTA POMOCI PRO UŽIVATELE

V případě, že uživatel potřebuje jakoukoliv pomoc či změnu týkající se:

- jeho počítače a jiného svěřeného ICT vybavení
  - nastavení systému
  - nastavení oprávnění
  - instalace a konfigurace SW
- nutnosti nahlásit událost
  - chybné fungování nebo porucha systému
  - bezpečnostní incident či podezření na něj
  - potenciální riziko pro společnost (zranitelné místo)
- otázek a nejasností k bezpečnosti informací apod.

může kontaktovat příslušné kontaktní místo**:**

- HelpDesk sekce ICT služby
  - Hotline (pracovní dny 7-16 hod) linka **4433**
  - portál ČEPS http://**/portalsap.e-ceps.cz/irj/portal**
- HelpDesk sekce EŘIS
  - řídí se provozní dokumentací sekce EŘIS
- Specialista bezpečnosti ICT Helena Urbančíková, linka **4832**
- Manažer bezpečnosti informací Jan Šmolík, linka **4794**
- Bezpečnostní ředitel (pouze v případě nedostupnosti předchozích nebo v krizové situaci) Martin Bílek, linka **4463.**

7 DESATERO UŽIVATELE

- **<u>Uživatel informačních systémů ČEPS musí:</u>**

1. *Znát své povinnosti a odpovědnosti uživatele IS/ICT ČEPS v oblasti informační bezpečnosti a dodržovat je.*
2. *Dodržovat požadavky na strukturu a četnost změny hesla a držet svoje autentizační údaje (hesla) v tajnosti.*
3. *Dodržovat pravidla pro klasifikaci a ochranu informací a práci s nimi.*
4. *Pro práci s informacemi a informačními systémy ČEPS používat pouze zařízení poskytnutá nebo schválená pro výkon této činnosti.*
5. *Ukládat informace na určených úložištích společnosti, kde jsou zabezpečena a zálohována.*
6. *Pracovat na své pracovní stanici nebo notebooku výhradně se schváleným SW, HW a nastavenou konfigurací.*
7. *Při práci s mobilními prostředky výpočetní techniky dbát maximální obezřetnosti a zamezit ztrátě nebo zcizení.*
8. *Dodržovat pravidla pro používání chytrých telefonů / tabletů*
9. *Oznámit na kontaktní místo jakýkoliv výskyt události, která je v rozporu s pravidly informační bezpečnosti.*
10. *Dodržovat zásady bezpečného chování a pravidla netikety při práci s Internetem a e-mailem.*