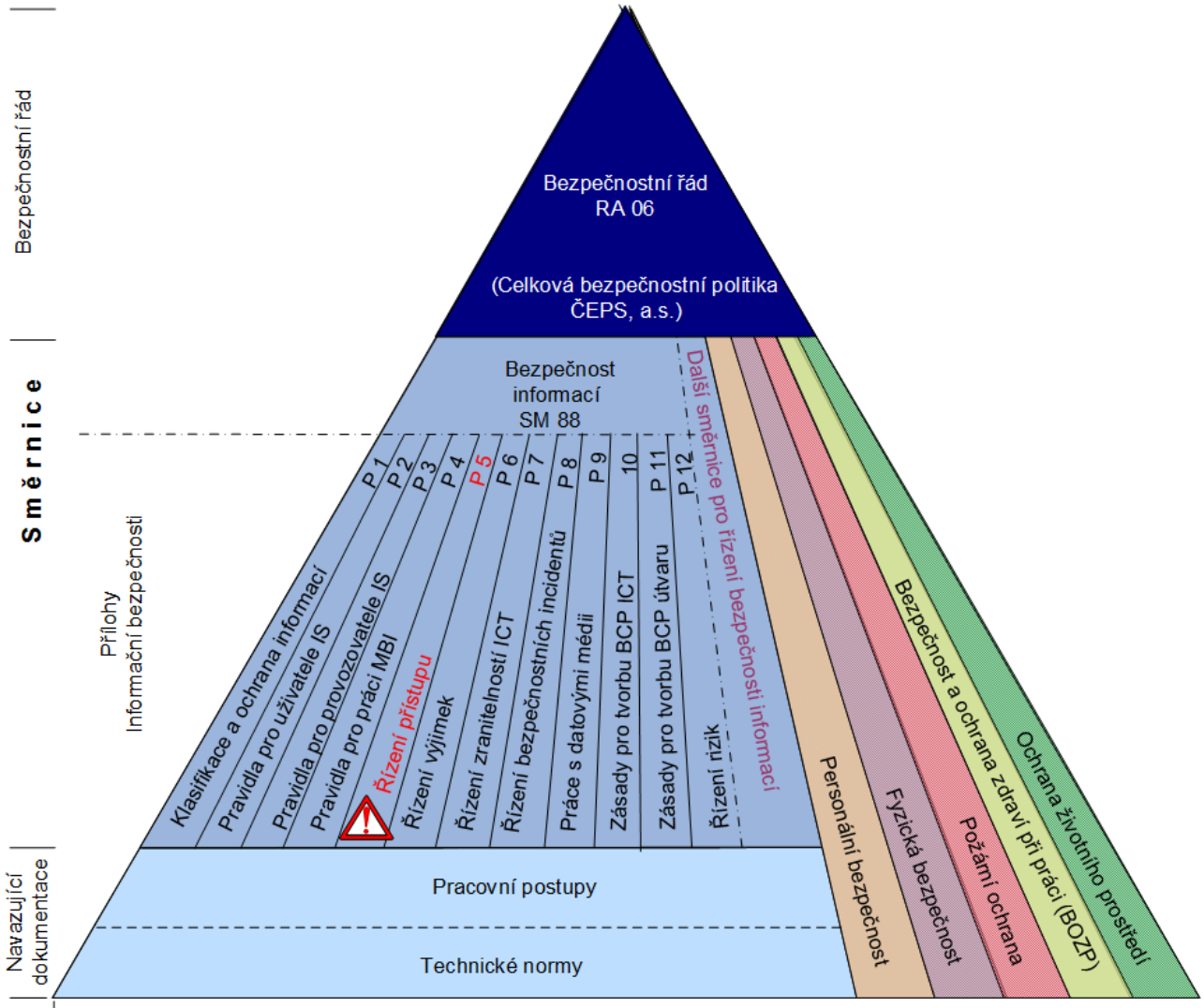
ŘÍZENÍ PŘÍSTUPU

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

Dokument „*Řízení přístupu"* je samostatnou přílohou směrnice *Bezpečnost informací* (dále „SM/88"), která stanovuje základní principy, pravidla a požadavky bezpečnosti informací. Tato příloha stanovuje pravidla, která určují postupy pro autorizaci, zřizování, změny a odebírání přístupových práv uživatelů, administrátorů a dalších specifikovaných rolí využívajících nebo podílejících se na zajištění provozu IS/ICT ČEPS. Příloha se nezabývá řízením fyzického přístupu, jehož pravidla jsou popsána ve směrnici SM/85.

Účelem řízení přístupu je zajistit přístup k informacím nebo informačním systémům pouze pro oprávněné (autorizované) uživatele nebo správce a zabránit tak neoprávněnému přístupu.

1.1 Role, odpovědnosti a pravomoci

Ředitelé sekcí Energetické řídící a informační systémy, ICT služby a Řízení provozu a údržby jsou v roli provozovatelů informačních systémů ČEPS ve své působnosti a odpovídají za zajištění:

- definici rolí a s nimi souvisejících standardních oprávnění,
- schvalování přístupů dle dále uvedených činností,
- výkon správy (administrace) systémů a práci oddělení HelpDesk v souladu s touto přílohou.

Vedoucí odboru Personalistika odpovídá za zajištění včasného předávání informací mezi odborem Personalistika[1], provozovateli IS a oddělení Strategie a bezpečnost ICT. Především odpovídá za zajištění předávání informací o:

- nástupech zaměstnanců, včetně informace o jejich pracovním zařazení,
- změnách v pracovním zařazení zaměstnanců,
- výstupech zaměstnanců a včas poskytnuté informaci o tom, že zaměstnanec je ve výpovědní lhůtě.

HelpDesk[2] slouží jako jednotné kontaktní místo provozovatelů IS i pro požadavky na zřizování a rušení přístupů. Vedoucí HelpDesku odpovídá za:

- předání požadavků na zajištění požadovaných přístupů a oprávnění na příslušné správce systémů[3] ve stanovených lhůtách.

Příslušné kontakty jsou uvedeny v kap. 5

Manažer bezpečnosti informací odpovídá za:

- schvalování přístupů dle specifikace uvedené dále v textu,
- provádění kontroly nad činnostmi řízení přístupových práv (zřizování, změny a odebírání),
- návrh opatření, které v případě porušení bezpečnosti vedou k ochraně společnosti
  - rušení přístupů, interních i vzdálených
  - monitoring zavedených opatření.

Oprávněný zaměstnanec ČEPS uvedený ve smlouvě s externím subjektem – odpovídá za:

- informování HelpDesku a manažera bezpečnosti informací o smluvních jednáních s externími subjekty v souvislosti s řízením přístupu,
- zajištění specifikace a odsouhlasení přístupových práv externích subjektů dle této přílohy,
- informování HelpDesku a manažera bezpečnosti informací o ukončení smluvního vztahu v souvislosti s řízením přístupu.

Vedoucí zaměstnanci odpovídají u svých podřízených za:

[1] Odbor Personalistika řeší standardní přístupy do IS ČEPS ve spolupráci se sekcí ICT služby. Přístup do systémů TRIS, DAMAS Energy a ŘS stanic PS řeší jejich provozovatel individuálně
[2] HelpDesk sekce „ICT služby" a HelpDesk „JIRA" pro potřeby systémů TRIS a DAMAS Energy
[3] Workflow zpracování požadavků v rámci sekce „ICT služby" se řídí interní dokumentací sekce

- schvalování žádosti o nadstandardní přístupy,
- pravidelnou kontrolu souladu přidělených oprávnění a pracovního zařazení,
- žádost o odebrání přístupů v odůvodněných případech (např. dlouhodobá pracovní neschopnost apod.).

Klíčový uživatel schvaluje přidělení rolí i mimo své podřízené, ale pouze za svou oblast (jako např. jednotlivé moduly v SAP).

2 DEFINICE ZÁKLADNÍCH POJMŮ A ZKRATEK

Autentizace - proces ověření (a tím i ustavení) identity v IS.

Autorizace přístupu k informacím - proces udělení (v negativním případě odepření) přístupu k informacím. Autorizovaný uživatel je uživatel, kterému bylo uděleno oprávnění k přístupu nebo patří do skupiny uživatelů, které přísluší oprávnění přístupu.

Dvoufaktorová autentizace – proces ověření identit, při kterém se využívá dvou způsobů ověření, obvykle tím co člověk „má“ (např. předmět s certifikátem) a tím, co člověk „zná“ (např. heslo).

„Need to know“ – princip, který říká, že zaměstnancům má být přidělován pouze přístup k informacím, které „potřebují znát“ pro výkon svých pracovních povinností.

Role – označení entity, které se přidělují konkrétní oprávnění, a která tak definuje úroveň přístupu.

Silná autentizace – proces ověření identity, při kterém se využívá dvou a více faktorů.

3 ŘÍZENÍ PŘÍSTUPU

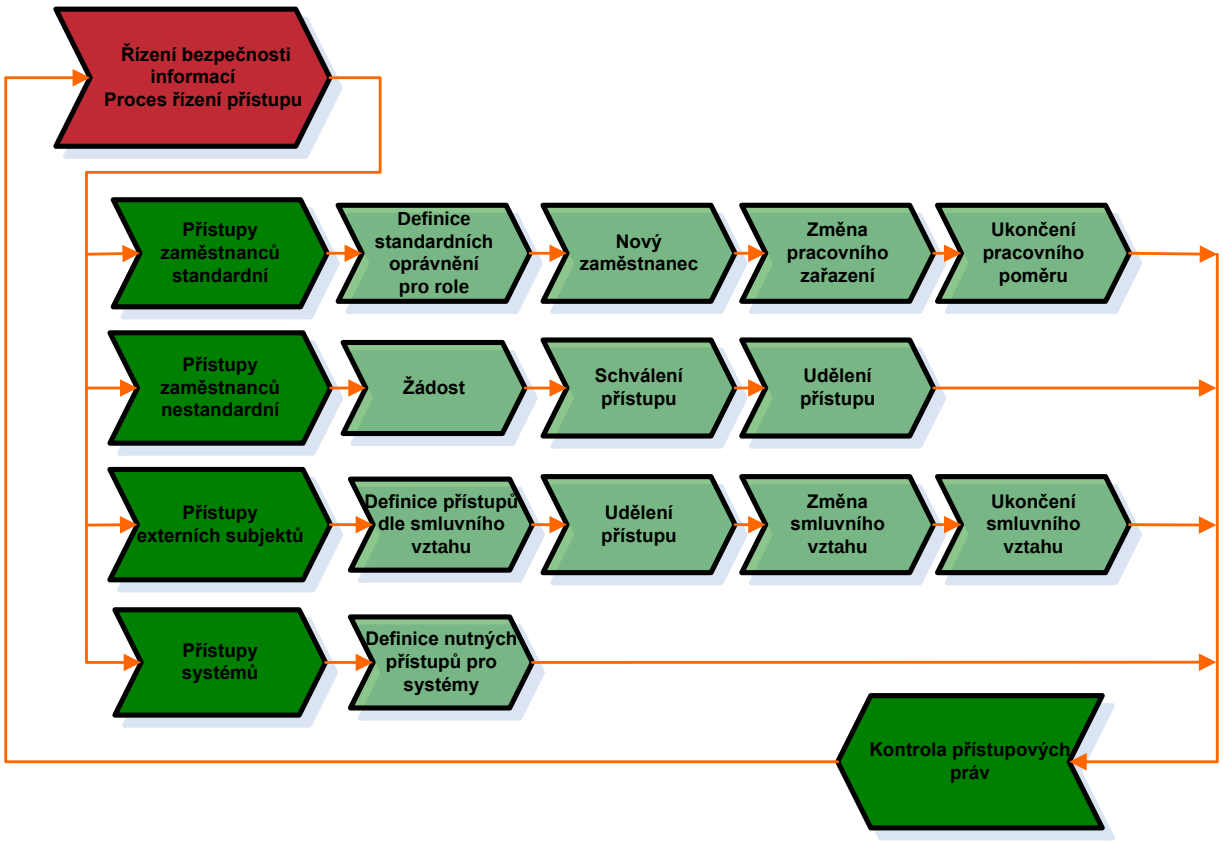
3.1 Události a činnosti při řízení přístupu

Pro řízení přístupu jsou klíčové události:

- nástup nového zaměstnance,
- změna pracovní pozice,
- ukončení pracovně právního vztahu,
- dlouhodobá pracovní neschopnost,
- potřeba přístupových práv nad rámec základních práv přiřazených dané roli (uživatele nebo administrátora),
- potřeba přístupových práv pro externí subjekty,
- potřeba přístupových práv pro systémy.

Na tyto události navazují související činnosti tak, aby byl přidělen přístup, který je potřebný pro výkon pracovních povinností:

- přístupy zaměstnanců – standardní,
- přístupy zaměstnanců – nadstandardní,
- přístupy externích subjektů,
- přístupy informačních systémů nebo aplikací,
- kontrola přístupových práv.



3.2 Přístupy zaměstnanců – standardní

Definice standardních oprávnění pro role

Pro každou pracovní pozici ve společnosti jsou stanoveny role (nebo kombinace rolí) v IS, které přísluší oprávnění nutná pro výkon pracovních povinností. Za specifikaci oprávnění pro role v informačním systému odpovídá jeho provozovatel.

Pravidla pro získání a správu certifikátu, pokud jej role vyžaduje, jsou specifikována ve směrnici SM/96 *Nákup, evidence a používání ICT vybavení* (stanovuje způsob nakládání uživatelů s hardwarovými a softwarovými produkty v IS ČEPS). Nároky na vzdálený přístup zaměstnanců do IS jsou definovány ve směrnici SM/103 *Nákup, evidence a používání ICT infrastruktury*.

Nástup nového zaměstnance

Odbor *Personalistika* informuje o nástupu nového zaměstnance a jeho pracovním zařazení (roli) sekci *ICT služby*, která zajistí standardní přístupy k IS.

Změna pracovního zařazení

O změně pracovního zařazení zaměstnance odbor *Personalistika* informuje sekci *ICT služby*, jejíž povinností je odebrat zaměstnanci stávající přístupová oprávnění a nastavit nová dle definice standardních oprávnění pro jeho novou pracovní roli.

Ukončení pracovního poměru

O ukončení pracovního poměru zaměstnance informuje odboru *Personalistika* na začátku výpovědní lhůty sekci *ICT služby*. Uvede se den ukončení pracovního poměru. Nadřízený pracovníka rozhodne o případných mimořádných bezpečnostních opatřeních v průběhu výpovědní lhůty. Navrhovaná mimořádná bezpečnostní opatření konzultuje přímý nadřízený zaměstnance s manažerem bezpečnosti informací a provozovatelem IS.
Taková opatření mohou zahrnovat:

- okamžité zrušení přístupu k vybraným informačním systémům a informačním zdrojům společnosti,
- odebrání možnosti vzdáleného přístupu a předmětů pro dvoufaktorovou autentizaci.

Sekce *ICT služby* zajistí realizaci mimořádných bezpečnostních opatření a zrušení nebo uzamknutí účtů zaměstnance ke dni ukončení jeho pracovního poměru. V odůvodněných případech může nadřízený zaměstnanec písemně požádat o odložení uzamknutí účtu odcházejícího zaměstnance. Žádost, která musí obsahovat důvod a termín požadovaného prodloužení platnosti, schvaluje manažer bezpečnosti informací.

3.3 Přístupy zaměstnanců – nadstandardní

Vyžaduje-li výkon pracovních povinností zaměstnance další přístupová oprávnění (mimo standardní), musí o jejich přidělení požádat provozovatele IS přímý nadřízený zaměstnance.
Požadavek na nadstandardní přístup musí být dále schválen provozovatelem IS, případně klíčovým uživatelem.

3.4 Přístupy externích subjektů

Udělení přístupu

Rozsah přístupových oprávnění pro externí subjekty musí být určen smlouvou, ve které musí být mj. stanoven postup, jak lze rozsah přístupů externího subjektu měnit. Veškeré přístupy (interní i vzdálené) a jejich rozsah eviduje a schvaluje provozovatel IS, kterého se přístup týká a manažer bezpečnosti informací před uzavřením smluvního vztahu.
O zřízení přístupových oprávnění žádá prostřednictvím aplikace HelpDesk oprávněný zaměstnanec ČEPS uvedený ve smlouvě s externím subjektem. Schválená žádost musí obsahovat specifikaci

přístupových oprávnění i dobu, na kterou se zřizují. Pokud je to technicky možné, přidělují se oprávnění pouze na dobu určitou, obvykle na dobu 12 měsíců (nejdéle však na dobu trvání smluvního vztahu). Vzory Žádosti o přístup externího subjektu k IS ČEPS a Prohlášení o seznámení se a porozumění SM/88 jsou uvedeny v dodatku.

Změna existujících přístupů

Při změně nebo doplnění smluvního vztahu oprávněný zaměstnanec ČEPS požádá prostřednictvím aplikace HelpDesk o změnu zřízených přístupových oprávnění stejným způsobem jako při udělení prvotního přístupu.

Ukončení přístupu

Není-li již přístup externího subjektu do IT prostředí nutný nebo při ukončení smluvního vztahu požádá oprávněný zaměstnanec ČEPS prostřednictvím aplikace HelpDesk o zrušení přístupových oprávnění.
Povinností správců příslušných systémů je zrušit či uzamknout přístupové účty ke dni ukončení smluvního vztahu nebo zkontrolovat jejich automatické ukončení nastavené v IS.

3.5 Přístupy informačních systémů nebo aplikací

Specifikace přístupů pro skripty, automatizované systémy nebo předávání dat mezi aplikacemi musí být řešeny také na principu „need to know“. Přístup systému k jinému systému, nebo vzájemné propojení systémů, aplikací a datových přenosů schvaluje provozovatel příslušného IS.

3.6 Kontrola přístupových práv

Administrátoři prostředků informačního systému, za které odpovídají, jsou povinni pravidelně provádět kontrolu přístupových oprávnění zaměstnanců. Administrátoři jsou dále povinni udržovat aktuální dokumentaci o přidělených rolích a pravidelně kontrolovat soulad přístupových práv s těmito rolemi. Pozornost nutno věnovat uživatelům, kteří již nejsou zaměstnanci společnosti, jsou dlouhodobě nepřítomni nebo mají přístupy zřízeny na základě smluvního vztahu. Na případné nekorektní přístupy musí administrátor okamžitě upozornit buď přímého nadřízeného zaměstnance nebo oprávněného zaměstnance ČEPS uvedeného ve smlouvě s externím subjektem a po dohodě tyto přístupy zrušit nebo zablokovat. Manažer bezpečnosti informací má právo provádět kontroly aktuálního stavu dokumentace přístupových práv pro každý klíčový IS, včetně namátkové kontroly souladu potřebných přístupových práv se skutečným stavem.

4 ZÁKLADNÍ PRAVIDLA ŘÍZENÍ PŘÍSTUPU

Ve výše popsaných činnostech řízení přístupu musí být dodržována jednotná pravidla vyplývající z provozních a bezpečnostních požadavků společnosti. Pro specifické nebo netypické informační systémy je možné obecná pravidla upravit při zachování následujících principů.

4.1 Obecné principy řízení přístupu

- uživatelům a administrátorům mohou být přidělena pouze oprávnění, která potřebují k vykonávání svých pracovních povinností při dodržování zásady „co není povoleno, je zakázáno“ a zásady „need to know“,
- každý uživatel IS ČEPS musí mít svůj vlastní jedinečný uživatelský účet, kterému jsou v jednotlivých systémech, modulech nebo aplikacích přiřazeny specifické role dle jeho pracovní náplně,

- zřizování skupinových uživatelských účtů nebo sdílení individuálních účtů je možné pouze v případech, kdy technologicky není možné vytvořit individuální účty pro všechny uživatele a musí být povoleno výjimkou z bezpečnosti informací (Příloha č. 6 SM/88),
- přístupová práva jsou jednotlivým rolím přiřazena na základě činností a odpovědností těchto rolí v systému nebo aplikaci,
- přístup k aktivům IS ČEPS může být povolen a nastavení realizováno pouze na základě:
  - přidělení přístupových práv a schválené sady základních přístupových práv pro role ve společnosti,
  - smluvního vztahu s externím subjektem a smluvně definovaných přístupových práv (žádost viz. kap. 5.2),
- pro přístup k OS a aplikacím musí být nastaveno (tam kde je to možné) časové omezení relace nebo spojení (např. automatické odhlášení uživatele, zamknutí konzole apod. – dle možností a způsobu využívání aplikace),
- žádosti pro nadstandardní přístup schválené oprávněnými osobami musí být evidovány a archivovány alespoň tři roky pro umožnění kontrol nebo vyšetřování bezpečnostních incidentů,
- přidělování privilegovaných[4] oprávnění musí být řízeno a minimalizováno na míru nezbytně nutnou pro provoz systému a uživatelé ani administrátoři nesmějí používat účty s privilegovanými oprávněními pro běžnou práci nesouvisející se správou IS,
- biometrické prostředky musí být při řízení přístupu použity v souladu s platnou právní úpravou (zejména zákonem č. 101/2000 Sb., o ochraně osobních údajů, v platném znění),
- vzdálené přístupy musí být realizovány v souladu se směrnicí SM/103 nebo schváleny manažerem bezpečnosti informací.

4.2 Řízení přístupu uživatelů

Zaměstnanci

Administrátoři mohou zaměstnancům zřídit nebo změnit uživatelský přístup, pokud byly splněny následující podmínky:

- jedná se o přidělení přístupových práv dle pracovního zařazení a s ním související schválené sady základních přístupových práv pro role,
- nestandardní přístup zaměstnance byl schválen příslušnou autoritou (nadřízený zaměstnance, klíčový uživatel a provozovatel IS) a existuje o tom písemný nebo elektronický zápis (žádost).

Uživatel stanice nesmí být jejím lokálním administrátorem. V případě, že je to z nějakého důvodu nutné (funkce atypické aplikace apod.), musí být schválena výjimka z bezpečnosti informací[5](Příloha č. 6 SM/88). Takový uživatel se pak stává správcem stanice a musí se při práci řídit touto přílohou. Uživatel s administrátorskými právy nesmí měnit schválenou konfiguraci pracovní stanice ani vypínat bezpečnostní software a musí zachovávat přístup pro globální skupinu Domain Admins.

[4] Privilegovaná oprávnění jsou taková oprávnění, která dávají uživateli (administrátor, supervisor…) možnost překonat některá systémová nebo aplikační opatření.

[5] Globální výjimku mají udělenu určení pracovníci sekcí „Energetické řídící a informační systémy“ a „ICT služby “, u kterých ji vyžaduje jejich pracovní náplň

Externí subjekty

Administrátoři mohou pracovníkům externích subjektů zřídit nebo změnit uživatelský přístup, pokud byly splněny následující podmínky:

- přístup externího subjektu byl schválen příslušnou autoritou (manažer bezpečnosti informací a provozovatel IS),
- existuje smluvní ujednání a písemný nebo elektronický zápis o typu a rozsahu přístupu a jeho schválení,
- vzdálený přístup je realizován pomocí standardní VPN s dvoufaktorovou autentizací.

Pokud je to nutné, smí být vytvořeny skupinové účty pro přístup pracovníků externího subjektu k systémům a zařízením.
Při nízké frekvenci využití přístupového účtu je vhodné udržovat účet primárně zablokovaný a uvolnit ho pouze na dobu nutnou pro provedení požadovaného zákroku. O tomto opatření rozhoduje provozovatel IS po dohodě s oprávněným zaměstnancem ČEPS uvedeným ve smlouvě s externím subjektem.

4.3 Řízení privilegovaného přístupu (administrátorský přístup)

Administrátoři jsou povinni:

- pro činnosti nesouvisející se správou používat svůj neprivilegovaný účet běžného uživatele.
- používat svůj jedinečný privilegovaný účet, nikoliv primární systémové skupinové účty (Administrators).
- pro jednotlivý administrační zásah používat příkazy pro spuštění aplikace s jinými právy, než je aktuální login (‘runas‘ resp. ‘sudo‘).
- účelně využívat všechny dostupné mechanismy pro řízení přístupu (např. ACL).
- využívat možnosti nastavovat práva ke zdrojům OS (např. práva zapisovat do registrů, skupina wheel u UNIX systémů apod.), pokud je takové nastavení účelné.
- připojovat se k serverům v DMZ pouze z DMZ nebo ze zóny se stejným nebo vyšším stupněm bezpečnosti.
- zajistit, aby k serverům v jejich správě nebylo možné přistupovat jinak, než definovaným a schváleným způsobem (dodržovat konfigurační standardy serverů.).

4.4 Správa hesel

Při konfiguraci systému administrátor nastavuje politiku pro tvorbu hesla, která v závislosti na typu účtu musí splňovat následující parametry:

Hesla k administrátorským účtům:

- délka hesla: min. 14 znaků,
- složení hesla: povinná kombinace malých a velkých písmen, číslic (min. 2 číslice) a speciálních znaků (min. 1 speciální znak),
- maximální doba platnosti hesla: 90 dnů,
- minimální počet hesel, která se nesmí opakovat za sebou: 5,
- maximální počet neúspěšných přihlášení, po kterém se uzamkne účet: 50,
- pokud dojde k uzamčení účtu z důvodu velkého počtu neúspěšných přihlášení, musí být účet uzamčen minimálně 5 minut nebo do zásahu administrátora.

Administrátoři jsou povinni používat pro šifrování hesel nejsilnější algoritmus, který je v distribuci systému dostupný a negativně neovlivní chod systému. Mohou však využít i silnější algoritmy dodávané mimo standardní distribuci systému.

Administrátoři jsou povinni umožnit či upřednostnit silnou autentizaci nebo dvoufaktorovou autentizaci, pokud je to technicky možné.

Hesla k uživatelským účtům:

- délka hesla: min. 8 znaků,
- složení hesla: povinná kombinace malých a velkých písmen, číslic a speciálních znaků,
- maximální doba platnosti hesla: 90 dnů,
- minimální počet hesel, která se nesmí opakovat za sebou: 5,
- maximální počet neúspěšných přihlášení, po kterém se uzamkne účet: 50,
- pokud dojde k uzamčení účtu z důvodu velkého počtu neúspěšných přihlášení, musí být účet uzamčen minimálně 5 minut nebo do zásahu administrátora.

Systémová hesla (pro skripty a automatizované systémy):

- délka hesla: min. 15 znaků,
- složení hesla: Povinná kombinace malých a velkých písmen, číslic a speciálních znaků,
- minimální počet hesel, které se nesmí opakovat za sebou: 10.

Neumožňuje-li systém výše uvedené požadavky naplnit, musí administrátor požádat o výjimku bezpečnosti informací a co nejvíce se k těmto parametrům přiblížit.

Povoleno je použití stejných hesel k serverům patřícím ke stejné službě a zpracovávajícím data stejné klasifikace.
Ve skriptech a automatizovaných systémech přístupu nesmí být hesla ukládána přímo v kódu v nechráněné (nešifrované) podobě. Pokud je to z technických důvodů nutné, musí být udělena výjimka bezpečnosti informací.

Ochrana hesla

Obecná pravidla pro ochranu hesel uživatelů specifikuje Příloha č. 2 SM/88.

Administrátoři jsou povinni přísně chránit svá hesla před kompromitací a minimalizovat rizika související s jejich vyzrazením.

Speciální administrátorská hesla (např. k recovery konsoli) musí být uložena v zalepené a podepsané obálce v trezoru příslušného nadřízeného.

Pokud je z provozních důvodů nezbytné předat nové heslo elektronickou cestou (mail, SMS), nesmí být společně uvedeny další identifikační údaje – tj. adresa/název aplikace a LoginID.

Pokud jsou administrátorská hesla ukládána v elektronické podobě, musí být využito zabezpečené úložiště. Zabezpečeným úložištěm se rozumí systém pro správu hesel, zaručující tyto vlastnosti úložiště:

- zaručení důvěrnosti hesel (hesla jsou v úložišti šifrována),
- zaručení integrity hesel (elektronický podpis, příp. hash),
- zaručení dostupnosti historických hesel (zálohování).

4.5 Řízení přístupu k zařízením, systémům a sítím

Pracovní stanice

Pro řízení přístupu uživatelů k pracovním stanicím musí být vytvořeny a aplikovány skupinové politiky Active Directory. Tyto politiky musí být součástí konfiguračních standardů.
Na pracovních stanicích včetně notebooků není povoleno sdílet celé disky nebo jednotlivé adresáře kromě standardního systémového sdílení. Uživatel může v případě potřeby požádat prostřednictvím

aplikace HelpDesk o vytvoření sdíleného prostoru na souborových serverech k tomu určených. Ve výjimečných případech mu může být povoleno krátkodobé sdílení adresářů lokálního diskového prostoru (nejdéle na 24 hodin). Toto sdílení nesmí být opakované a přístup smí být umožněn pouze konkrétním doménovým uživatelům či skupinám (nesmí být použity obecné skupiny jako Everyone, Users apod.).
Na uživatelských stanicích je zakázáno sdílení tiskáren.

Servery a síťová zařízení

Na serverech a síťových zařízeních nesmí být uživatelům povoleno přihlášení k systému. Uživatelé se mohou přihlašovat pouze ke službám, které jsou serverem nebo zařízením nabízeny podle provozní dokumentace a účelu zařízení.

Servery a síťová zařízení v DMZ

Uživatelé se mohou k serverům a síťovým zařízením v DMZ přihlašovat pouze prostřednictvím schválených aplikací a nástrojů (SM/103).

Servery zpracovávající nebo uchovávající „CITLIVÉ INTERNÍ“ informace

Uživatelé se mohou k serverům s informacemi klasifikovanými bezpečnostním klasifikačním stupněm „CITLIVÉ INTERNÍ“ přihlašovat pouze prostřednictvím k tomu určených aplikací a nástrojů.

Vzdálené přístupy

Vzdálený přístup do sítí společnosti je povolen pouze schválenou technologií, VPN přístup musí být realizován alespoň dvoufaktorovou autentizací.
Uživatelé i administrátoři mohou využívat vzdálených přístupů k síti na základě jejich pracovních povinností a kompetencí a to pouze s využitím schválených mobilních komunikačních prostředků společnosti. Přístup musí být buď standardní (SM/103) nebo musí být schválen manažerem bezpečnosti informací a provozovatelem IS.

Princip oddělení v sítích

Topologie počítačových sítí a jejich segmentace musí být popsána v dokumentaci provozovatelů IS. Tato dokumentace musí být udržována aktuální. Administrátoři musí při své práci dodržovat všechna ustanovení této dokumentace.

Citlivé systémy společnosti musí být provozovány odděleně. Týká se to především dispečerského řídicího systému TRIS, obchodního systému DAMAS Energy a pracoviště Homebankingu. Požadavek na oddělení systému v sítích ČEPS dává provozovatel IS a manažer bezpečnosti informací. Vyžadují-li tyto systémy komunikovat s okolím, musí být perimetr systému odpovídajícím způsobem zajištěn a zdokumentován.

5 DODATKY

5.1 Vzor žádosti o udělení přístupu do IS ČEPS

ŽÁDOST O UDĚLENÍ PŘÍSTUPU

Přístup externího subjektu k IS ČEPS

Žádost o udělení přístupu k IS ČEPS, a.s., pro zaměstnance externího subjektu uplatňuje žadatel - zaměstnanec ČEPS / ČEPS Invest oprávněný ze smluvního vztahu s externím subjektem.

Žádost o udělení přístupu k IS ČEPS, a.s., pro zaměstnance externích subjektů musí obsahovat:

(pro každý doménový účet je nutné zvlášť vyplnit tyto údaje):

Jméno a příjmení: (společnost):		
Požadavek na domovský adresář uživatele: (disk H:\)	☐ ANO	☐ NE
Požadavek na přístup k dalším síťovým zdrojům : (např. K:\,T:\,V:\)	☐ ANO	☐ NE
- Upřesnění požadovaného přístupu, kam:		
Požadavek na e-mailovou schránku uživatele: (@ceps.cz, @cepsinvest.cz)	☐ ANO	☐ NE
Požadavek na vzdálený přístup do IS (VPN):	☐ ANO	☐ NE
- Upřesnění požadovaného přístupu, kam: - Typ komunikace, protokol: - Posouzení rizik (klasifikace informací): *Kontaktní osoba pro VPN:* - e-mail: - mobilní telefon:		
Požadavek na přístup k portálu SAP EP:	☐ ANO	☐ NE
Požadavek na licenci SAP:	☐ ANO	☐ NE
- Odpovědná osoba definující požadovaný rozsah oprávnění:		
Stručný popis činnosti v IS:		
Požadovaný termín platnosti oprávnění k přístupu: (čl. 3.4, P5, SM/88)	Od:	Do:
Odpovědná osoba (žadatel):		
Číslo smlouvy:		

Různé:	

5.2 Žádost o udělení vzdáleného přístupu k ŘS stanic PS ČEPS

Celý proces udělování přístupů k systému vzdálených přístupů k ŘS stanic PS je popsán v pracovním postupu PP 66 „***Postup pro schvalování, zakládání a přístup uživatele Systému vzdálených přístupů k řídicím systémům a ochranám stanic PS ČEPS, a.s.“***

PROHLÁŠENÍ

Přístup externího subjektu k IS ČEPS

5.3 Vzor prohlášení

Jméno a příjmení:
(Společnost)

prohlašuji, že jsem byl/byla dnešního dne náležitě seznámen/seznámena se směrnicí **SM/88** ***Bezpečnost informací*** a jejími přílohami:

č. 1 ***Klasifikace a ochrana informací a práce s nimi***

č. 2 ***Pravidla bezpečnosti informací pro uživatele IS*** *)

č. 3 ***Pravidla bezpečnosti informací pro provozovatele a administrátora IS*** *)

č. 5 ***Řízení přístupu*** *)

Obsahu rozumím a jsem si plně vědom/vědoma svých závazků, které pro mne z těchto bezpečnostních pravidel vyplývají.

V …….. dne:……..

……..
podpis

Školení provedl: …….

**) nehodící se škrtněte*

5.4 Kontaktní místa pro řízení přístupu

HelpDesk ICT služby:		http://**portalsap.e-ceps.cz/irj/portal**
TRIS:	Bohuslav Podroužek	e-mail: podrouzek@ceps.cz
DAMAS Energy:	Jiří Rýznar	e-mail: ryznar@ceps.cz