BEZPEČNOSTNÍ PŘÍRUČKA UŽIVATELE ICT

KÓD	MP-2/2015
VERZE	3.1
TYP	Metodický pokyn
ČÍSLO JEDNACÍ	ČP/77173/2023/CKA/02
NAHRAZUJE VNITŘNÍ PŘEDPIS	MP-2/2015 – verze 3.0
KLASIFIKACE	Interní
PLATNOST OD	11. 12. 2023
ÚČINNOST OD	15. 12. 2023
GARANT	Ing. Jaroslav Hloušek ředitel úseku ICT a eGovernment podepsáno elektronicky dne 11. 12. 2023
SCHVALOVATEL	schváleno garantem – technická revize

Obsah

1. Úvodní ustanovení

1.1. Účel

(1) Metodický pokyn je vydán v souladu se směrnicí SM-1/2015 Bezpečnostní politika ICT a zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a navazujících právních předpisů v aktuálním znění.

(2) Bezpečnostní příručka uživatele ICT (dále jen „Příručka“) stanovuje povinnosti uživatele a základní bezpečnostní postupy při práci s ICT České pošty, s.p. (dále jen „ČP“).

(3) Použití vlastních zařízení v ICT ČP je zakázáno. Výjimky schvaluje Bezpečnostní manažer ICT (manažer specializovaného útvaru ICT bezpečnost).

1.2. Působnost

(1) Příručka je závazná pro všechny uživatele, tzn. zaměstnance České pošty, s.p. (dále jen „ČP“) i uživatele externích dodavatelů a partnerů, kteří v rámci své pracovní činnosti mají přístup k informacím ČP a využívají služeb ICT ČP. Seznámení externích subjektů s povinnostmi uživatele a základními bezpečnostní postupy při práci s ICT ČP (viz příloha č. 2 - Bezpečnostní požadavky pro přístup pracovníků externích subjektů k ICT ČP – školicí materiál) zajistí garant externího subjektu evidovaný v rámci registrace externího uživatele v IDM.

(2) Rozsah uživatelských oprávnění je nadřízeným nebo garantem externího uživatele požadován a schvalován principem „need to know“, tedy jsou přidělována pouze taková uživatelská oprávnění, která jsou nezbytná a účelná pro plnění pracovních nebo smluvních povinností uživatele. Schvalovatelé jsou povinni přidělená oprávnění pravidelně kontrolovat a v případě chybného přidělení zajistit nápravu.

(3) Rozsah povinností a postupy při práci v informačním systému nakládající s utajovanými informacemi dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, definují směrnice SM-3/2014 Projektová bezpečnostní dokumentace informačního systému pro zpracování utajovaných informací, SM-4/2014 Provozní bezpečnostní směrnice – Správce IS a SM-5/2014 Provozní bezpečnostní směrnice – Uživatel IS.

(4) ICT systémy ČP, slouží pouze pro účely související s pracovním poměrem a uživatel bere na vědomí, že zaměstnavatel (ČP) je spravuje a má k nim řízený přístup. Do uživatelského e-mailu je ze strany zaměstnavatele přístup možný pouze v mimořádných a odůvodněných případech. Zaměstnavateli tak mohou být zobrazena případná soukromá data či komunikace zaměstnance zaslaná jiným subjektem. Tyto mimořádné a odůvodněné případy jsou uvedené v kapitole 6 této příručky.

1.3. Přehled změn proti předchozí verzi

Oproti verzi 3.0 došlo k následujícím změnám:

Změna názvu aplikace Skype pro firmy na Webex.
Úprava názvu (původně Bezpečnostní příručka uživatele ICT ČP).
Přílohy označené jako samostatné dostupné na IntraNetu ČP.
Formální úpravy.

1.4. Zkratky a pojmy

ZKRATKY	
IDM	Identity management (slouží ke správě uživatelů a jejich oprávnění).
POJMY	
Autentizace	Prokázání identity uživatele, zdroje nebo zařízení.
Bezpečnost informací	Zachování důvěrnosti, integrity a dostupnosti informací a dalších vlastností jako např. odpovědnost, nepopiratelnost a spolehlivost.
Bezpečnostní incident	Událost nebo události, které ohrožují bezpečnost informací, případně porušení bezpečnostních požadavků.
Dostupnost	Znamená, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby.
Důvěrnost	Znamená, že informace jsou přístupné nebo sděleny pouze těm, kteří jsou k tomu oprávněni.
Elektronická komunikace	On-line přenos informací v elektronické podobě. Zahrnuje např.: e-mail, Webex, chat, obdobná on-line komunikace a sociální sítě.
Chráněná informace	Informace, která na základě rozhodnutí příslušné autority (vlastníka informace) musí být chráněna, protože její zpřístupnění, modifikace, zneužití, zničení nebo ztráta by mohlo poškodit nebo ohrozit zájmy ČP, a/nebo způsobit ČP nebo jinému subjektu újmu (materiální i nemateriální).
Informační a komunikační technologie (ICT)	Veškerá technika, která se zabývá zpracováním a přenosem informací, a to je zejména výpočetní a komunikační technika a programové vybavení (např. firemní aplikace, e-mail, cloudová a interní úložiště, Webex atd.)
Integrita	Znamená zajištění správnosti a úplnosti informací.
Klasifikace informací	Definování kategorie informace z hlediska jejího významu a povahy. Podle stanovené kategorie se určuje konkrétní způsob její ochrany.
Mobilní zařízení ICT ČP	Přenosný elektronický přístroj s různým programovým vybavením jako např. mobilní telefon, notebook, netbook, smartbook, PDA, tablet, USB zařízení apod.
Monitorování	Sledování, dozor, kritické pozorování nebo určování stavu pro identifikování odchylek od požadované nebo očekávané úrovně.
Nepříznivá událost	Jakákoliv událost, která vede nebo může vést k narušení bezpečnosti nebo činností ČP.
Příručka	Bezpečnostní příručka uživatele ICT ČP, tzn. tento dokument.
Uživatel	Každá fyzická osoba (zaměstnanec ČP nebo smluvně pověřený zaměstnanec externí fyzické nebo právnické osoby), které byl přidělen přístup k ICT ČP a příslušná přístupová oprávnění. Pro účely této příručky se jedná o uživatele ICT ČP.

2. Povinnosti uživatele

(1) Chránit informace a ICT systémy ČP, se kterými se dostane do kontaktu při výkonu své pracovní činnosti, před případným zneužitím, poškozením, zničením nebo ztrátou.

(2) Chránit informace v listinné i elektronické podobě v ICT v souladu s ustanoveními uvedenými ve směrnici SM-5/2013 Ochrana informací.

(3) Používat pouze schválené postupy a nástroje (např. certifikáty vydané certifikační autoritou, schválený SW) k elektronické ochraně informací.

(4) Chránit zařízení a data ICT před poškozením, zničením, ztrátou nebo zneužitím. Zejména uzamykáním kanceláří a pracovních prostor a vždy při odchodu z pracoviště uzamknutím pracovní plochy počítače (stisknutím Win+L nebo Ctrl+Alt+Delete -> uzamknout) nebo odhlášením ze systému.

(5) Používat dostatečně silná hesla podle níže uvedených zásad:

a) Heslem nebo jeho součástí nesmí být jméno uživatele nebo jeho blízkých, číslo průkazu, název organizační jednotky, pracoviště, pošty a jiné známé, nebo snadno zjistitelné informace, nejčastěji používaná hesla, hesla na základě mnohonásobně opakujících se znaků (3 a více), přihlašovací jména e-mailu, názvy systémů nebo obdobný způsob tvorby hesla.

b) Délka hesla musí být minimálně 12 znaků, u privilegovaných účtů (například administrátoři, servisní účty, …) musí být 17 znaků (nedoporučuje se používat české znaky s diakritikou a písmena Y a Z), doporučuje se používat hesla delší, a kombinaci malých velkých písmen a číslic, případně speciálních znaků (např: */!{@).

c) V případě, kdy délka hesla z technických důvodů nemůže být minimálně 12 znaků (17 znaků u privilegovaných účtů), musí heslo obsahovat minimálně jedno velké písmeno (A-Z), malá písmena (a-z) a číslice (0-9). Dále je nutno v tomto případě využít maximální možnou délku hesla. Tyto případy (výjimky) schvaluje Bezpečnostní manažer ICT.

d) Heslo nesmí uživatel sdílet s jiným uživatelem.

e) Platnost hesla je nastavena na maximálně 200 dnů.

f) Změněné heslo nesmí být shodné s předchozími hesly.

(6) Chránit autentizační a přístupové údaje (hesla, klíče apod.) před vyzrazením, ztrátou nebo zneužitím a v žádném případě je nikomu nesdělovat. V případě, že k prozrazení dojde, musí být autentizační a přístupové údaje okamžitě změněny.

(7) Věnovat pozornost podezřelému chování lidí i ICT systémů, systémovým oznámením a hlášením bezpečnostních programů jako je například antivirová ochrana. Při zjištění nebo i jen podezření na zavirování či podezřelé chování, neprodleně toto oznámit na ServiceDesk a dále se řídit jeho pokyny.

(8) Provést antivirovou kontrolu na všech záznamových médiích (celého záznamového média nebo jen datového souboru) při obdržení od externích subjektů. Při předávání záznamových médií externímu subjektu je uživatel povinen zabezpečit, aby na daném záznamovém médiu byly pouze informace určené pro daný externí subjekt.

(9) Nezasahovat do systémového nastavení jednotlivých zařízení ICT ani neprovádět instalaci programů. (netýká se k tomu určených pracovníků).

(10) Nekopírovat SW na jiný počítač nebo jej předávat jiné osobě v rámci nebo mimo ČP.

(11) Bez souhlasu nadřízeného nepřemisťovat jednotlivá zařízení ICT mimo určené prostory a dodržovat provozní řád daného pracoviště.

(12) Pracovat se zařízením ICT tak, aby chráněné informace nemohly být odposlechnuty, odpozorovány nebo vyčteny ze zpracovávaných dokumentů a obrazovek zařízení ICT jinou nepovolanou osobou.

(13) Aktivně se účastnit školení bezpečnosti ICT.

(14) V případě žádosti operačního systému o restartování zařízení ICT (např. PC), v co nejkratší době ukončit veškerou činnost a restart provést.

(15) Hlásit zjištěné bezpečnostní incidenty (viz kapitola 7 této příručky a kapitola 10 směrnice SM-1/2015 Bezpečnostní politika ICT).

(16) Hlásit zjištěné mimořádné události Stálé operační službě na telefonní číslo 605 225 555, které je také uvedeno v krizové kartě provozovny v souladu s metodickým pokynem MP-7/2022 Stálá operační služba (Informační systém pro řešení mimořádných událostí). Jedná se zejména o narušení nebo zničení důležitých zabezpečovacích zařízení, výpadek dodávky elektrické energie spojený s vyřazením elektronických systémů.

3. Uživateli je zakázáno

(1) Přerušovat probíhající aktualizace systému, vypínat antivirovou ochranu nebo měnit konfiguraci bezpečnostních prvků ochrany ICT.

(2) Bez předchozího souhlasu Bezpečnostního manažera ICT a povolení nadřízeného vedoucího zaměstnance používat zařízení pro svou osobní potřebu, instalovat jakýkoli SW, manipulovat s ICT ČP jinak než povoleným způsobem, snažit se měnit HW komponenty či systémovou konfiguraci nebo připojovat vlastní (soukromá) zařízení nebo zařízení ve vlastnictví jiných (cizích) firem.

(3) Pracovat s cizími autentizačními nebo přístupovými údaji.

(4) Využívat chybně přidělená oprávnění, která uživateli nepřísluší.

(5) Využívat internetové služby a elektronickou komunikaci k jiným než pracovním účelům.

(6) Přesměrovávat služební e-mail na soukromé e-maily zaměstnanců (například zřízený e-mail u poskytovatelů: seznam.cz, gmail.com, Hotmail.com, outlook.cz, …) nebo e-maily zřízené u externích firem.

4. Záznamová média

(1) Záznamová média používaná v ČP jsou vyjímatelné pevné disky, USB zařízení (např. flashdisk, externí disky), DVD, CD, magnetické pásky, případně další. Jejich ochranu a označování popisuje směrnice SM-5/2013 Ochrana informací.

(2) Záznamová média musí být uživatelem před likvidací nebo opakovaným použitím kontrolována, zda neobsahují chráněné informace nebo licencované programové vybavení.

(3) Záznamová média obsahující chráněné informace musí být před opakovaným použitím jiným uživatelem bezpečně smazána přepsáním speciálním softwarovým produktem znemožňující obnovu původních

informací. Speciální softwarové produkty stanovuje a schvaluje Bezpečnostní manažer ICT. Seznam je zveřejněn na IntraNetu ČP (Odborné úseky > ICT > Bezpečnost ICT).

(4) Likvidace chráněných informací uložených na záznamových médiích musí být provedena bezpečným smazáním speciálním softwarovým produktem, viz odst. (3) této kapitoly, nebo skartací samotného záznamového média podle směrnice SM-5/2013 Ochrana informací.

5. Pravidla používání elektronické komunikace

(1) Uživatelé smějí využívat pouze určené přidělené prostředky elektronické komunikace.

(2) Chráněné informace mohou být systémy elektronické komunikace přenášeny pouze v souladu se směrnicí SM-5/2013 Ochrana informací.

(3) Prostředky elektronické komunikace jsou určeny primárně ke služebním účelům a její využití k mimopracovním účelům může být vedoucími zaměstnanci na úrovni řízení G-1 povolena výjimečně, se zachováním pravidel etického vystupování a s vyloučením případného konfliktu zájmů tak, aby tato komunikace nemohla být zneužita proti zájmům ČP.

(4) Uživatelé jsou povinni si počínat opatrně při otevírání zpráv elektronické komunikace a jejich příloh, zejména těch, které přicházejí od neznámých odesílatelů.

(5) Přesměrování e-mailu na e-mailové adresy xxx.yyy@cpost.cz je povoleno. Přesměrování provádí uživatel sám po dohodě se zaměstnancem, na kterého e-mail přesměruje. Pokud uživatel nemůže nastavit přesměrování sám, může nadřízený požádat prostřednictvím ServiceDesku o nastavení automatické odpovědi s náhradním kontaktem. Podrobný popis činností je uveden v příloze č. 1.

(6) Nedostupnost e-mailu z důvodu ukončení pracovního poměru je automaticky zajištěna jeho zablokováním, tzn. odesílatel obdrží automatickou odpověď o nedostupnosti e-mailové adresy.

(7) V rámci používání elektronické komunikace je uživateli zakázáno:

a) Pokoušet se použít účty jiných uživatelů.

b) Vědomě odesílat zprávy se soubory obsahující škodlivý kód (viry, trojské koně apod.).

c) Vytvářet falešné zprávy, hlavičky ve zprávách apod., za účelem falšování identity odesílatele.

d) Rozesílat nepožadované zprávy či obtěžovat jiným způsobem (např. frekvence nebo velikost zpráv).

6. Specifikace přístupu zaměstnavatele k e-mailu

6.1. Specifikace závažných důvodů

(1) Při zpracování služebních e-mailů je v závažných případech možné provést kontrolu a odpovídající reakci ze strany ČP.

(2) Závažnými důvody (odůvodněné případy) jsou zejména:

a) Dlouhodobá nepřítomnost zaměstnance (nemoc apod.),
b) ukončení pracovního poměru zaměstnance,
c) podezření na zneužívání pracovního e-mailu pro soukromé účely,
d) podezření na bezpečnostní incident,
e) podezření na páchání trestné činnosti,
f) podezření na nekalé jednání,
g) jiné podezření, při jehož naplnění by zaměstnavatel nebo jiná osoba mohla utrpět vážnou újmu na svých právech.

6.2. Pravidla pro přístup k e-mailu uživatele

(1) Při přístupu k e-mailu uživatele v odůvodněných případech musí být zajištěno soukromí a oprávněné zájmy zaměstnance, do jehož e-mailu je přistupováno. Přistoupit k e-mailu lze až tehdy, kdy není možné postupovat pro zajištění zaměstnavatelových práv jiným způsobem, nezasahujícím do soukromí zaměstnance. Tedy, za splnění uvedeného předpokladu a současně při závažných důvodech dle kapitoly 6.1, je možno zajistit přístup k e-mailu zaměstnance jiným, k tomu pověřeným a k tomu odborně způsobilým zaměstnancem, který zajistí její vyhodnocení a zpracování. Zaměstnance pověřuje nadřízený zaměstnance užívajícího e-mailovou schránku.

(2) Žádost o přístup k e-mailu podává v odůvodněných případech zpravidla nadřízený zaměstnance cestou ServiceDesku. Pokud není žadatelem, musí být o přístupu informován.

(3) Nadřízený zaměstnance je povinen o skutečnosti, že byl proveden přístup k e-mailu, zaměstnance neprodleně informovat, a to po provedeném přístupu a se sdělením zjištěných skutečností.

(4) Požadavek k přístupu k e-mailu ze závažných důvodů dle kapitoly 6.1., odst. (2), písm. c), e) a g) může podat zaměstnanec útvaru bezpečnost, který zajistí i následné šetření daného podezření.

(5) Požadavek k přístupu k e-mailu ze závažných důvodů dle kapitoly 6.1., odst. (2), písm. f) je oprávněn podat Compliance Officer ČP, který zajistí i následné šetření daného podezření v souladu s příslušným vnitřním předpisem.

(6) Požadavek k přístupu k e-mailu může dát v případě podezření na bezpečnostní incident Bezpečnostní manažer ICT.

(7) Osoba, která přistoupila k e-mailu v souladu s tímto předpisem, při vyhodnocení a zpracování jejího obsahu musí dodržet veškerá bezpečnostní ustanovení této příručky, především pak mlčenlivost o všech zjištěných skutečnostech a ochranu soukromí dotčeného zaměstnance.

(8) Požadavky na přístup ze závažných důvodů k e-mailu jsou zaznamenány a archivovány v ServiceDesku.

(9) V případě ukončení pracovního poměru zaměstnance je e-mail neprodleně zablokován a do 30 dnů od ukončení pracovního poměru smazán.

7. Bezpečnostní incident

7.1. Základní bezpečnostní incidenty

(1) Projev počítačového viru nebo jiného škodlivého SW.

(2) Nestandardní chování zařízení ICT nebo uživatelů.

(3) Kompromitace nebo zneužití autentizačních a přístupových údajů (např. hesla), podezření nebo pokus o kompromitaci (např. podvodné e-maily, neúmyslné prozrazení hesla apod.).

(4) Ztráta nebo odcizení zařízení ICT, mobilního zařízení ICT nebo záznamového média.

(5) Proniknutí nepovolané osoby na pracoviště uživatele, k zařízení ICT nebo i pokus o něj.

(6) Výstražné hlášení operačního systému nebo aplikačního SW indikující porušení bezpečnosti.

(7) Neoprávněná změna HW, SW nebo konfigurace.

(8) Ztráta důvěrnosti informací zapříčiněná například chybným nastavením oprávnění, kompromitací nebo zneužitím autentizačních údajů, nebo ztrátou či odcizením zařízení ICT.

(9) Chybně přidělená oprávnění nad rámec mu svěřených pracovních povinností.

7.2. Řešení bezpečnostního incidentu

(1) Každý bezpečnostní incident nebo podezření na něj musí uživatel neprodleně oznámit na ServiceDesk, případně přes svého nadřízeného, který incident oznámí na ServiceDesk.

(2) Uživatel je povinen poskytnout věcně příslušným organizačním jednotkám nezbytnou součinnost při šetření a řešení bezpečnostního incidentu. Na základě vyhodnocení bezpečnostního incidentu specializovaný útvar ICT bezpečnost provede potřebná opatření pro uvedení ICT systému ČP do bezpečného stavu.

(3) Zvládání bezpečnostních incidentů řeší metodický pokyn MP-15/2019 Zvládání bezpečnostních incidentů.

8. Zvládání nepříznivých událostí

8.1. Základní typy nepříznivých událostí

(1) Oblast fyzické bezpečnosti:

a) Oheň, kouř nebo výbuch,
b) záplavy nebo prosakování kapalin,
c) narušení konstrukce budovy,
d) přírodní katastrofa,
e) narušení fyzické ochrany interních prostor.

(2) Oblast bezpečnosti ICT:

a) Porucha HW,

b) narušení aplikačního prostředí ČP, chyby SW, narušení integrity dat (chyby v datech, chybějící předepsané náležitosti),

c) výpadek elektrického proudu.

8.2. Povinnosti uživatele při vzniku nepříznivých událostí

(1) V případě vzniku nepříznivých událostí, které mohou způsobit narušení činností a dopady na ČP, má každý zaměstnanec povinnost poskytnout nezbytnou součinnost pro jejich zvládání.

(2) Uživatel informuje nadřízeného a řídí se jeho pokyny a dokumenty, které popisují zvládání nepříznivých událostí. Uživatel sleduje informační zdroje sloužící ke zvládání nepříznivých událostí – IntraNet ČP (pokud je to možné).

(3) Uživatel je povinen postupovat podle směrnice SM-6/2015 Zajištění bezpečnosti a ochrany zdraví při práci a směrnice SM-12/2013 Zajištění požární ochrany.

(4) Uživatel je povinen v případě, kdy je schopen situaci zvládnout, provést nezbytná opatření k minimalizaci dopadů na ICT ČP, ochranu informací v něm zpracovávaných a ČP obecně. Provedení opatření je uživatel povinen oznámit nadřízenému.

(5) Uživatel je povinen veškeré nepříznivé události neprodleně hlásit na ServiceDesk ČP, a to včetně již provedených opatření.

8.3. Požár

(1) Vyhlásit požární poplach a řídit se příslušnou požární poplachovou směrnicí pracoviště.

(2) V rámci možností a stavu situace zabezpečit záznamová média a zařízení s chráněnými informacemi proti zničení nebo ztrátě.

8.4. Havárie ústředního topení, vodovodního nebo kanalizačního řádu

(1) Informovat o havárii nadřízeného a zodpovědnou osobu správy objektu.

(2) Provést nezbytná opatření k minimalizaci dopadů pro ICT.

8.5. Havárie zařízení ICT ČP

(1) Neodstraňovat závady zařízení ICT vlastními prostředky.

(2) Informovat nadřízeného a závadu nahlásit na ServiceDesk.

9. Sankce

Porušení ustanovení tohoto dokumentu a souvisejících bezpečnostních politik, navazujících metodických pokynů a příruček a na základě posouzení závažnosti, míry zavinění, případně míry dopadu, a následků tohoto porušení (bezpečnostního incidentu) může být považováno za porušení povinnosti vyplývající z právních předpisů vztahujících se k zaměstnancem vykonávané práci se všemi důsledky z toho vyplývajícími.

10. Přechodná a závěrečná ustanovení

(1) Výklad a aktualizaci této příručky zajišťuje Bezpečnostní manažer ICT a jím pověřené osoby.

(2) Kontrolovat a ověřovat dodržování ustanovení tohoto metodického pokynu je oprávněn Bezpečnostní manažer ICT.

11. Související dokumenty a další informační zdroje

INTERNÍ	
SM-1/2015	Bezpečnostní politika ICT
MP-3/2015	Generická systémová bezpečnostní politika ICT
MP-15/2019	Zvládání bezpečnostních incidentů
SM-5/2013	Ochrana informací
MP-7/2022	Stálá operační služba (Informační systém pro řešení mimořádných událostí)
SM-6/2015	Zajištění bezpečnosti a ochrany zdraví při práci
SM-12/2013	Zajištění požární ochrany
SM-3/2014*	Projektová bezpečnostní dokumentace informačního systému pro zpracování utajovaných informací
SM-4/2014*	Provozní bezpečnostní směrnice – Správce IS
SM-5/2014*	Provozní bezpečnostní směrnice – Uživatel IS
SM-8/2013	Ochrana osobních údajů
SM-7/2015	Systém compliance v ČP a Podnikový compliance program proti korupci a dalším formám nekalého jednání
SM-8/2015	Oznamování a řešení podezření na nekalé jednání
EXTERNÍ	
zákon č. 181/2014 Sb.	o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
vyhláška č. 82/2018 Sb.	o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
DALŠÍ INFORMAČNÍ ZDROJE	
IntraNet ČP	Odborné úseky > ICT > Bezpečnost ICT

* Předpisy jsou k dispozici u specializovaného útvaru bezpečnost poštov. provozu. Jedná se o stupeň utajení „Obchodní tajemství“.

12. Seznam příloh

ČÍSLO PŘÍLOHY	NÁZEV
1. samostatná	Přesměrování e-mailu
2. samostatná	Bezpečnostní požadavky pro přístup pracovníků externích subjektů k ICT ČP – školicí materiál

Přílohy č. 1 a 2 jsou uveřejněny na IntraNetu ČP (Odborné úseky > ICT > Bezpečnost ICT). Za jejich obsah, uveřejnění a aktualizaci odpovídá Bezpečnostní manažer ICT a jím pověřené osoby.

Příloha č. 1 k MP-2/2015-verze 3.0

Přesměrování e-mailu

(1) **Automatické přesměrování emailové pošty mimo prostředí ČP je zakázáno.** Důvodem jsou rizika spojená se ztrátou důvěrnosti firemních i osobních informací.

(2) **Automatické přesměrování emailové pošty při ukončení pracovního poměru se standardně neprovádí**. Důvodem je možná ztráta důvěrnosti informací osobního charakterů, které mohou do schránky přijít a které uživatel nemůže ovlivnit. Navíc dle GDPR by byl nutný souhlas uživatele, který nelze jednoduše a prokazatelně získat.

(3) **Uživatel sám může** po dohodě s nadřízeným **nastavit automatickou odpověď o ukončení pracovního poměru a odkázat na jiného příjemce.** (obdobně jako při dovolené)

(4) **Nadřízený uživatele může požádat o nastavení automatické odpovědi při ukončení pracovního poměru za uživatele.** Doporučujeme však zvážit zda je to nutné a nepostačí standardní odpověď emailového systému o neexistenci emailové adresy.

(5) **Emailová schránka se po ukončení pracovního poměru udržuje funkční pro příjem emailů po dobu 7 dnů. Po uplynutí této doby emailové systémy emailovou komunikaci odmítnou jako nedoručitelnou standardní odpovědí.** V tomto případě je na odesilateli, aby zajistil řádné zaslání informací na funkční adresu ČP.

(6) V závažných důvodech, které by měly závažný dopad na ČP, může o jiném nastavení rozhodnout Bezpečnostní manažer ICT. Žadatel však musí zajistit, aby nedošlo k porušení legislativních požadavků na ochranu osobních údajů.

Příloha č. 2 k MP-2/2015 - verze 3.0

Bezpečnostní požadavky pro přístup pracovníků externích subjektů k ICT ČP – školící materiál

1. Úvodní ustanovení

(1) Pracovníkem externího subjektu se pro účely tohoto materiálu rozumí každá fyzická osoba vykonávající smluvní činnost pro externí subjekt, vyžadující uživatelský či administrátorský přístup do ICT ČP.

(2) Bezpečnostní požadavky pro přístup pracovníků externích subjektů k ICT ČP (dále požadavky) stanovují požadavky na přístupu pracovníků externích subjektů k ICT ČP za účelem plnění smluvního ujednání a jsou zpracovány v souladu s Bezpečnostní politikou ICT ČP a zákonem č.181/2014 Sb., o kybernetické bezpečnosti a navazujících legislativních předpisů v aktuálním znění.

(3) Rozsah uživatelských oprávnění se přiděluje principem „need to know“, a proto jsou přidělována pouze taková uživatelská oprávnění, která jsou nezbytná pro plnění pracovních povinností smluvního partnera.

(4) Žádost o zřízení přístupu předkládá zástupce externího subjektu prostřednictvím stanoveného zástupce ČP (stanovuje vedoucí organizačního celku ČP, v jehož gesci je externí subjekt smluvně vázán) nebo stanoveného projektového manažera a schvalování probíhá v souladu s interními předpisy ČP.

(5) Seznam proškolených osob, které jsou vzhledem ke svým předdefinovaným právům a privilegiím oprávněny využívat přístup k ICT ČP, vede stanovený zástupce ČP nebo projektový manažer ČP. Vzor seznamu je uveden v příloze.

(6) V případě, že seznámení pracovníků externích subjektů s povinnostmi uživatele a základními bezpečnostní postupy při práci s ICT ČP provádí externí subjekt podle školícího materiálu ve své gesci, zasílá seznam proškolených osob stanovenému zástupci ČP nebo projektovému manažerovi ČP.

(7) ČP si vyhrazuje právo auditovat smluvní povinnosti nebo právo nechat provést tyto audity třetí stranou, možnost monitorovat činnost externích subjektů a vyšetřovat bezpečnostní incidenty i v prostředí externího subjektu.

(8) Terminologie použitá níže v textu vychází z Bezpečnostní politiky ICT ČP.

2. Povinnosti pracovníků externích subjektů

(1) Chránit informace v listinné nebo elektronické podobě, ICT systémy ČP i ICT systémy externího subjektu, se kterými se dostane do kontaktu při výkonu své pracovní činnosti, před případným zneužitím, poškozením, zničením nebo ztrátou.

(2) Používat bezpečná hesla podle níže uvedených zásad (pokud to systémy umožňují):

a) heslem nebo jeho součástí nesmí být jméno uživatele nebo jeho blízkých, číslo průkazu, název organizační jednotky, pracoviště, pošty a jiné známé, nebo snadno zjistitelné informace, nejčastěji používaná hesla, hesla na základě mnohonásobně opakujících se znaků (3 a více), přihlašovací jména e-mailu, názvy systémů nebo obdobný způsob tvorby hesla.

b) délka hesla musí být minimálně 12 znaků, u privilegovaných účtů (například administrátoři, servisní účty, …) musí být 17 znaků (nedoporučuje se používat české znaky s diakritikou a písmena Y a Z), doporučujeme se používat hesla delší, a kombinaci malých velkých písmen a číslic, případně speciálních znaků (např: */!{@)

c) v případě, kdy délka hesla z technických důvodů nemůže být minimálně 12 znaků (17 znaků u privilegovaných účtů), musí heslo obsahovat minimálně jedno velké písmeno (A-Z), malá písmena

(a-z) a číslice (0-9)). Dále je nutno v tomto případě využít maximální možnou délku hesla. Tyto případy (výjimky) schvaluje Bezpečnostní manažer ICT.

d) heslo nesmí uživatel sdílet s jiným uživatelem,
e) platnost hesla je u zařízení ICT ČP nastavena na maximálně 200 dnů,
f) změněné heslo nesmí být shodné s 12 předchozími hesly.

(3) Chránit autentizační a přístupové údaje (hesla, klíče apod.) před vyzrazením, ztrátou nebo zneužitím a v žádném případě je nikomu nesdělovat. V případě že k prozrazení dojde, musí být autentizační a přístupové údaje okamžitě změněny.

(4) Věnovat pozornost podezřelému chování lidí, ICT systémům ČP i ICT systémům externích subjektů, systémovým oznámením a hlášením bezpečnostních programů, jako je například antivirová ochrana. Při zjištění incidentu nebo i jen podezření na ně neprodleně toto oznámit na ServiceDesk ČP (tel. 800 260 026) a dále se řídit jeho pokyny.

(5) Bez souhlasu ČP nepřemisťovat zařízení ČP mimo určené prostory a dodržovat provozní řád daného pracoviště ČP.

(6) Pracovat tak, aby chráněné informace nemohly být odposlechnuty, odpozorovány nebo vyčteny ze zpracovávaných dokumentů a obrazovek jinou nepovolanou osobou. Za chráněné informace ČP definuje všechny informace, které vznikly v souvislosti s činnostmi ČP a pro ČP vyjma informací, které je možno považovat za veřejně dostupné informace.

(7) Účastnit se organizovaných školení bezpečnosti ICT pořádaných ČP.

(8) Hlásit zjištěné bezpečnostní incidenty.

(9) Zajistit součinnost při výkonu práva auditovat plnění smluvní povinností ze strany ČP a to i v případě, je-li audit prováděn třetí stranou, případně při vyšetřování bezpečnostního incidentu.

3. Je zakázáno

(1) Přerušovat probíhající aktualizace systémů ICT ČP, vypínat antivirovou ochranu nebo měnit konfiguraci bezpečnostních prvků ochrany ICT ČP.

(2) Bez souhlasu ČP používat ICT ČP pro svou osobní potřebu, instalovat jakýkoli SW, manipulovat s ICT ČP jinak než povoleným způsobem, snažit se měnit HW komponenty či systémovou konfiguraci nebo připojovat vlastní (soukromá) zařízení pracovníků externího subjektu. Pracovní zařízení externího subjektu smí být připojeno pouze se souhlasem ČP.

(3) Pracovat s cizími autentizačními a přístupovými údaji.

(4) Využívat chybně přidělená oprávnění, která pracovníkům externího subjektu nepřísluší.

4. Záznamová média

(1) Pracovníkům externích subjektů je zakázáno zpracovávat chráněné informace ČP na záznamových médiích, která nejsou vlastnictvím ČP. Ochranu a označování záznamových médií ČP řeší směrnice ČP SM-5/2013 Ochrana informací.

5. Změnové řízení

(1) Každá změna software či jeho konfigurace (kromě standardních operátorských činností) v ICT ČP musí být zaznamenána v provozní dokumentaci systému.

(2) Každá verze programového vybavení uvolněná pro nasazení musí být uložená včetně zdrojových kódů, podpůrného programového vybavení, dokumentace a testovacích protokolů. Každá tato verze musí nést informaci o čase a místě nasazení. Verze programového vybavení musí být externím subjektem uchovány nejméně 3 roky po ukončení používání dané verze programového vybavení v provozu.

(3) Významnější změny, které by mohly ovlivnit dostupnost nebo integritu dat (např. upgrade nebo změna aplikace), musí být před schválením ověřeny v testovacím prostředí a to i z hlediska dopadu na bezpečnost informací. Pro všechny změny v jednotlivých částech ICT ČP musí existovat procedura návratu do stavu před změnou.

6. Zvládání bezpečnostních incidentů

(1) Základní bezpečnostní incidenty v prostředí ICT ČP i ICT externího subjektu:

a) projev počítačového viru nebo jiného zlomyslného SW,

b) nestandardní chování zařízení,

c) kompromitace nebo zneužití autentizačních a přístupových údajů (např. hesla), podezření na ně,

d) ztráta nebo odcizení zařízení nebo záznamového média,

e) proniknutí nepovolané osoby na pracoviště k zařízení nebo i pokus o něj,

f) výstražné hlášení operačního systému nebo aplikačního SW,

g) neoprávněná změna HW, SW nebo konfigurace,

h) neúmyslné nebo úmyslné vyzrazení chráněných informací.

(2) Řešení bezpečnostního incidentu:

a) Každý bezpečnostní incident se musí neprodleně oznámit na ServiceDesk ČP (tel. 800 260 026).

b) Pracovníci externích subjektů jsou povinni poskytnout odborným útvarům ČP (specializovaný útvar ICT bezpečnost, útvar ICT provoz) nezbytnou součinnost.

c) Specializovaný útvar ICT bezpečnost provede potřebná opatření podle vyhodnocení bezpečnostního incidentu pro uvedení ICT systému ČP do bezpečného stavu.

7. Zvládání mimořádných událostí

(pracovníci externích subjektů mají fyzický přístup do prostředí ČP)

(1) Základní typy mimořádných událostí:

a) Oblast fyzické bezpečnosti v prostředí ČP:

- oheň, kouř nebo výbuch,
- záplavy nebo prosakování kapalin,
- narušení konstrukce budovy,
- přírodní katastrofa.

b) Oblast bezpečnosti ICT ČP:

- porucha HW,
- narušení aplikačního prostředí ČP, chyby SW, narušení integrity dat (chyby v datech, chybějící předepsané náležitosti),
- výpadek elektrického proudu.

(2) Povinnosti při vzniku mimořádných událostí:

a) V případě vzniku mimořádných událostí, které mohou způsobit narušení činností a dopady na ČP nebo externí subjekt, má každý povinnost poskytnout nezbytnou součinnost pro jejich zvládání.

b) Pracovníci externích subjektů jsou povinni veškeré mimořádné události v oblasti fyzické bezpečnosti neprodleně hlásit stálé operační službě ČP na číslo 605 225 555 a to včetně již provedených opatření a v oblasti bezpečnosti ICT ČP na ServiceDesk ČP (tel. 800 260 026).

c) V případě závady zařízení ICT ČP závadu neodstraňovat vlastními prostředky, ale závadu nahlásit na ServiceDesk ČP (tel. 800 260 026).

8. Sankce

Porušení ustanovení bezpečnostních politik a interních předpisů ČP na základě posouzení závažnosti, míry zavinění, případně míry dopadu, a následků tohoto porušení (bezpečnostního incidentu) může být považováno za porušení povinností vyplývajících ze smluvního ujednání se všemi právními důsledky včetně odpovědnosti za vzniklou újmu a/nebo povinnosti zaplatit sjednanou smluvní pokutu.

9. Související dokumenty

a) SM-1/2015 – verze 3.0 – Bezpečnostní politika ICT

b) MP-2/2015 – verze 3.0 – Bezpečnostní příručka uživatele ICT ČP

10. Závěrečné ustanovení

Výklad a aktualizaci těchto požadavků zajišťuje ČP (specializovaný útvar ICT bezpečnost). Pracovníci externích subjektů potvrzují svým podpisem proškolení v oblasti bezpečnosti ICT ČP.

Seznam proškolených pracovníků externího subjektu Příloha

Datum školení	Externí subjekt	Příjmení a jméno (hůlkovým písmem)	Podpis	Přístup do systémů ČP	Klasifikace informací

V rámci školení je předán školící materiál.