příloha č. 15

Česká pošta

Metodický pokyn

Identifikace	MP-2/2015	Číslo jednací	ČP/5368/2015/GŘ
Nahrazuje		Klasifikace	Interní
Platnost	15. 1. 2015	Účinnost	1. 2. 2015

Bezpečnostní příručka uživatele ICT ČP

Verze 1.0

Podpis	
Datum	6. 8. 2014
Garant dokumentu	Ing. Pavel Chyla v. r.
Funkce	Vrchní ředitel divize ICT a eGovernment

Podpis		Podpis	
Datum	8. 10. 2014	Datum	15. 1. 2015
Garant dokumentu	Jan Přerovský v. r.	Schvalovatel	Ing. Martin Elkán v. r.
Funkce	Ředitel OZ ICTs	Funkce	generální ředitel

Dokument je řízen správcem řídicích dokumentů ČP a platná verze je dostupná na podnikovém portálu ČP, po vytištění se výtisk stává neřízeným dokumentem.

Obsah dokumentu

Evidence revizí a změn

Verze	Účinnost od	Důvod a popis změny	Autor	Schválil
Verze 1.0	1.2.2015	Základní dokument	Milan Konečný	Petr Slavík

1. Úvodní ustanovení

(1) Bezpečnostní příručka uživatele ICT ČP (dále příručka) je vydána v souladu se směrnicí Bezpečnostní politika ICT ČP.

(2) Příručka stanovuje povinnosti uživatele ICT ČP a základní bezpečnostní postupy při práci s ICT ČP.

(3) Použití vlastních zařízení v ICT ČP je zakázáno. Výjimky schvaluje bezpečnostní manažer ICT (vedoucí odboru bezpečnost ICT). Definice bezpečnostních požadavků pro použití vlastních zařízení zaměstnanců ČP nebo externích subjektů v ICT ČP bude řešena v metodickém pokynu „Bezpečnostní politika BYOD ČP".

(4) Příručka je závazná pro všechny zaměstnance České pošty, s.p. (dále ČP), externí pracovníky ČP a externí subjekty, kterým byl povolen přístup k ICT ČP.

2. Základní pojmy a názvosloví užívané v ICT

(1) Terminologie použitá v této příručce vychází z Bezpečnostní politiky ICT.

(2) **Autentizace** – je prokázání identity uživatele, zdroje nebo zařízení.

(3) **Bezpečnost informací** – znamená zachování důvěrnosti, integrity a dostupnosti informací a dalších vlastností jako např. autentičnost, odpovědnost, nepopiratelnost a spolehlivost.

(4) **Bezpečnostní incident** – je událost nebo události, které ohrožují bezpečnost informací, případně porušení bezpečnostních politik nebo navazujících řídících dokumentů.

(5) **BYOD (Bring Your Own Device)** – je využívání vlastních zařízení pro pracovní účely a přístup k datům a aplikacím ČP.

(6) **Dokument** – je každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové či elektronické (digitální), která byla vytvořena v rámci ČP, nebo byla ČP doručena.

(7) **Dostupnost** – znamená, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby.

(8) **Důvěrnost** – znamená, že informace jsou přístupné nebo sděleny pouze těm, kteří jsou k tomu oprávněni.

(9) **Chráněná informace** – je informace, která na základě rozhodnutí příslušné autority (vlastník informačního aktiva) musí být chráněna, protože její zpřístupnění, modifikace, zničení nebo ztráta by způsobilo někomu nebo něčemu znatelnou újmu a škodu. Viz také směrnice SM-5/2013 Ochrana informací.

(10) **ICT (informační a komunikační technologie)** - je veškerá technika, která se zabývá zpracováním a přenosem informací, a to je zejména výpočetní a komunikační technika a její programové vybavení.

(11) **Integrita** – znamená zajištění správnosti a úplnosti informací.

(12) **Klasifikace informací** – je definování kategorie informace z hlediska jejího významu a povahy. Podle stanovené kategorie se určuje konkrétní způsob její ochrany.

(13) **Mobilní zařízení ICT ČP** – je malý přenosný elektronický přístroj s různým programovým vybavením jako např. mobilní telefon, notebook, netbook, smartbook, PDA, tablet, USB zařízení apod.

(14) **Monitorování** – je sledování, dozor, kritické pozorování nebo určování stavu pro identifikování odchylek od požadované nebo očekávané úrovně.

(15) **Oprávněná osoba** - je fyzická nebo právnická osoba, která splňuje podmínky přístupu nebo je oprávněna seznamovat se s příslušnou kategorií informace.

(16) **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.

3. Povinnosti uživatele ICT ČP

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

(2) Chránit informace nelistinného charakteru v ICT ČP v souladu s ustanoveními uvedenými ve směrnici SM-5/2013 Ochrana informací.

(3) Používat pouze schválené nástroje (např. certifikáty vydané certifikační autoritou) k elektronické ochraně informací.

(4) Chránit zařízení ICT ČP před poškozením, zničením, ztrátou nebo zneužitím uzamykáním kanceláří nebo pracovních prostorů a při odchodu z pracoviště uzamknout pracovní plochu počítače (stisknutím Win+L nebo Ctrl+Alt+Delete) nebo se odhlásit ze systému.

(5) Používat bezpečná hesla podle níže uvedených zásad (pokud to systém ICT ČP umožňuje):

a) heslo musí obsahovat nejméně velké písmeno (A-Z), čtyři malá písmena (a-z), číslici (0-9) a k zvýšení kvality hesla je doporučeno používat i speciální znaky (např. !, ?, *, +, apod.),

b) heslem nebo jeho součástí nesmí být jméno uživatele nebo jeho blízkých, číslo jeho průkazu, organizační jednotky, pracoviště, pošty apod.,

c) délka hesla musí být minimálně 8 znaků (nedoporučuje se používat české znaky s diakritikou a písmena Y a Z),

d) heslo nesmí uživatel sdílet s jiným uživatelem,

e) platnost hesla je u zařízení ICT ČP nastavena na 90 dnů,

f) změněné heslo nesmí být shodné s 12 předchozími hesly.

(6) Chránit autentizační a přístupové údaje (hesla, klíče apod.) před vyzrazením, ztrátou nebo zneužitím a v žádném případě je nikomu nesdělovat.

(7) Věnovat pozornost systémovým oznámením a hlášením bezpečnostních programů jako je například antivirová ochrana. Při zjištění nebo jen podezření na přítomnost počítačového viru vypnout zařízení ICT ČP a neprodleně to oznámit na ServiceDesk a dále se řídit jeho pokyny.

(8) Provést antivirovou kontrolu informací 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 ČP ani provádět instalaci programů.

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

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

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

(13) Účastnit se organizovaných školení bezpečnosti ICT.

(14) Hlásit zjištěné bezpečnostní incidenty (viz kapitola 6. této příručky a kap. 11. směrnice Bezpečnostní politika ICT).

4. Uživateli ICT ČP je zakázáno

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

(2) Bez souhlasu vedení 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.

(3) Pracovat s cizími autentizačními a přístupovými údaji.

(4) Zneužívat internetových služeb a emailu k jiným než služebním účelům.

5. Záznamová média

(1) Záznamová média používaná v ČP jsou vyjímatelné HDD, USB zařízení, DVD, CD, magnetické pásky, případně další. Jejich označování řeší 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 v sekci Bezpečnost ICT.

6. Bezpečnostní incident

6.1. Základní seznam bezpečnostních incidentů:

a) projev počítačového viru nebo jiného zlomyslného SW,

b) nestandardní chování zařízení ICT ČP,

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

d) ztráta zařízení ICT ČP, mobilního zařízení ICT ČP nebo záznamového média,

e) proniknutí nepovolané osoby na pracoviště uživatele, k zařízení ICT ČP 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.

6.2. Řešení bezpečnostního incidentu

(1) Každý bezpečnostní incident musí uživatel neprodleně oznámit na ServiceDesk ČP, případně svému nadřízenému.

(2) Uživatel je povinen poskytnout odboru bezpečnost ICT nezbytnou součinnost. Odbor bezpečnost ICT provede potřebná opatření podle vyhodnocení bezpečnostního incidentu pro uvedení ICT ČP do bezpečného stavu.

7. Havarijní situace

7.1. Základní typy havarijních situací:

(1) Oblast fyzické bezpečnosti

a) oheň, kouř nebo výbuch,

b) záplavy nebo prosakování kapalin,

c) narušení konstrukce budovy,

d) přírodní katastrofa.

(2) Oblast bezpečnosti ICT

a) porucha HW,

b) chyby SW,

c) výpadek elektrického proudu.

7.2. Postup uživatele při vzniku havarijních situací

(1) Uživatelé jsou povinni postupovat podle směrnice SM-30/2008 Zajištění bezpečnosti a ochrany zdraví při práci a směrnice SM-12/2013 Zajištění požární ochrany.

(2) Uživatel je pak povinen v případě, že je schopen situaci zvládnout, provést nezbytná opatření k minimalizaci dopadů pro ICT ČP a chráněné informace v něm zpracovávané.

(3) Po provedení nezbytných opatření je uživatel povinen oznámit nadřízenému vznik mimořádné situace a opatření, která provedl.

7.2.1. Požár

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

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

7.2.2. Havárie ústředního topení, vodovodního řádu, kanalizačního řádu či jiná obdobná havárie

Informovat o havárii nadřízeného a zodpovědnou osobu správy objektu.

7.2.3. Havárie zařízení ICT ČP

(1) Neodstraňovat závady zařízení ICT ČP vlastními prostředky.

(2) Informovat nadřízeného a závadu nahlásit na ServiceDesk ČP.

8. Sankce

Porušení ustanovení bezpečnostních politik a navazujících metodických pokynů a příruček na základě posouzení závažnosti, míry zavinění, případně míry dopadu, a následků tohoto porušení (bezpečnostního incidentu) může být považováno za porušení povinností vyplývajících z interních dokumentů ČP se všemi pracovněprávními důsledky v podobě upozornění na porušení povinností vyplývajících z právních předpisů vztahujících se k zaměstnancem vykonávané práci, ústního napomenutí nebo skončení pracovního poměru.

9. Související dokumenty

a) SM-1/2015 Bezpečnostní politika ICT

b) SM-5/2013 Ochrana informací

c) SM-30/2008 Zajištění bezpečnosti a ochrany zdraví při práci

d) SM-12/2013 Zajištění požární ochrany

10. Závěrečné ustanovení

Výklad a aktualizaci této příručky zajišťuje bezpečnostní manažer ICT ČP.