Příloha č. 11

Bezpečnostní příručka uživatele ICT ČP

1. Úvodní ustanovení

1.1. Bezpečnostní příručka uživatele ICT ČP - partner (dále příručka) je vydána v souladu s Bezpečnostní politikou ICT ČP a zákonem č.181/2014 Sb., o kybernetické bezpečnosti a navazujících legislativních předpisů v aktuálním znění.

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

1.3. Použití vlastních zařízení v ICT ČP je zakázáno. Výjimky schvaluje pracovník ČP - vedoucí odboru bezpečnost ICT (bezpečnostní manažer ICT).

1.4. Příručka je závazná pro uživatele ICT, kteří v rámci své pracovní činnosti mají přístup k informacím ČP a využívají služeb ICT ČP.

1.5. 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.

1.6. Elektronická pošta domény CPOST.CZ slouží pro účely komunikace související s pracovními činnostmi partnera se zaměstnanci ČP a partner bere na vědomí, že ČP má do emailových schránek domény CPOST.CZ v odůvodněných případech (viz kapitola 6 níže) přístup, a ČP by mohla být zobrazena i případná soukromá korespondence partnera v doméně CPOST.CZ.

2. Základní pojmy a názvosloví užívané v ICT

Terminologie použitá v této příručce vychází z Bezpečnostní politiky ICT ČP.

2.1. Autentizace – je prokázání identity uživatele, zdroje nebo zařízení.

2.2. Bezpečnost informací – znamená zachování důvěrnosti, integrity a dostupnosti informací a dalších vlastností jako např. autentičnost, odpovědnost, nepopiratelnost a spolehlivost.

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

2.4. 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 partnera, nebo byla ČP nebo partneru doručena.

2.5. Dostupnost – znamená, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby.

2.6. Důvěrnost – znamená, že informace jsou přístupné nebo sděleny pouze těm, kteří jsou k tomu oprávněni.

2.7. Chráněná informace – je informace, která na základě rozhodnutí původce (zpracovatel dokumentu) musí být chráněna, protože její zpřístupnění, modifikace, zničení nebo ztráta by způsobilo někomu nebo něčemu znatelnou újmu a škodu.

2.8. 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.

2.9. Integrita – znamená zajištění správnosti a úplnosti informací.

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

2.11. Monitorování – je sledování, dozor, kritické pozorování nebo určování stavu pro identifikování odchylek od požadované nebo očekávané úrovně.

2.12. Mimořádná událost – událost, která vede nebo může vést k narušení činností ČP nebo partnera.

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

2.14. ServiceDesk - organizační jednotka pro podporu funkcí a řešení problémů v rámci ICT ČP.

2.15. Uživatel – každá fyzická osoba (smluvní partner), které byl přidělen přístup k ICT ČP a příslušná přístupová oprávnění.

2.16. Schránka na jméno – je taková schránka elektronické pošty (e-mail), která je určena pouze pro pracovní účely partnera.

3. Povinnosti uživatele ICT ČP

3.1. Chránit informace v listinné nebo elektronické podobě a ICT systémy ČP, se kterými se dostane do kontaktu při výkonu své pracovní činnosti, před případným zneužitím, poškozením, zničením nebo ztrátou.

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

3.3. Chránit zařízení ICT ČP před poškozením, zničením, ztrátou nebo zneužitím uzamykáním kanceláří a pracovních prostorů a vždy při odchodu z pracoviště uzamknout pracovní plochu počítače nebo se odhlásit ze systému.

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

a) heslo musí obsahovat nejméně jedno 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 průkazu, organizační jednotky, pracoviště, pošty a jiné známé, nebo snadno zjistitelné informace,
c) délka hesla musí být minimálně 8 znaků (nedoporučuje se používat české znaky s diakritikou a písmena Y a Z), doporučujeme však používat hesla delší,
d) heslo nesmí uživatel sdílet s jiným uživatelem,
e) platnost hesla je u zařízení ICT ČP nastavena na maximálně 90 dnů,
f) změněné heslo nesmí být shodné s 12 předchozími hesly.

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

3.6. 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 neprodleně to oznámit na ServiceDesk a dále se řídit jeho pokyny.

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

3.8. Nezasahovat do systémového nastavení jednotlivých zařízení ICT ČP ani neprovádět instalaci programů.

3.9. Nekopírovat SW na jiný počítač nebo jej předávat jiné osobě v rámci nebo mimo partnera.

3.10. Bez souhlasu ČP nepřemisťovat zařízení mimo určené prostory a dodržovat provozní řád daného pracoviště.

3.11. 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.

3.12. Účastnit se organizovaných školení bezpečnosti ICT pořádaných ČP.

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

3.14. Hlásit zjištěné bezpečnostní incidenty (viz kapitola 7 této příručky).

3.15. Hlásit zjištěné mimořádné události stálé operační službě ČP na číslo 605 225 555. Jedná se zejména o narušení nebo zničení důležitých zabezpečovacích zařízení, výpadek dodávky elektrické energie spojený s vyřazením elektronických systémů a krádež nebo vloupání.

4. Uživateli ICT ČP je zakázáno

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

4.2. 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.

4.3. Pracovat s cizími autentizačními a přístupovými údaji.

4.4. Využívat chybně přidělená oprávnění, která uživateli nepřísluší.

4.5. Využívat internetové služby a emaily k jiným než pracovním účelům.

5. Záznamová média

5.1. Záznamová používaná média jsou vyjímatelné HDD, USB zařízení (flashdisk, externí HDD, ...), DVD, CD, magnetické pásky, případně další a musí se chránit proti neoprávněnému přístupu k informacím na nich uložených. Jejich ochranu a označování řeší směrnice ČP SM-5/2013 Ochrana informací.

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

5.3. 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 ČP.

6. Elektronická pošta

6.1. Specifikace závažných důvodů

6.1.1. V rámci zpracování elektronické pošty je nutné zajistit kontrolu, příjem a odpovídající reakci na zprávy související s pracovními činnostmi partnera v rámci ČP i v případech, kdy partner toto nemůže zajistit sám a to ze závažných důvodů.

6.1.2. Závažnými důvody (odůvodněné případy) jsou zejména:

a) Dlouhodobá nepřítomnost (např. nemoc).

b) Ukončení smluvního ujednání.

c) Podezření na zneužívání pracovního emailu pro soukromé účely.

d) Podezření na kybernetický bezpečnostní incident

e) Podezření na páchání trestné činnosti.

f) Jiné podezření, při jehož naplnění by ČP, partner nebo jiná osoba mohla utrpět vážnou újmu na svých právech.

6.2. Přístup k schránce elektronické pošty

6.2.1. V případech závažných důvodů je nutno zajistit přístup a zpracování došlé (a to i budoucí) pošty smluvního partnera pověřeným zaměstnancem ČP, který zajistí její vyhodnocení a zpracování.

6.2.2. Pověřený zaměstnanec ČP, je-li to možné, si vyžádá souhlas smluvního partnera předmětné schránky elektronické pošty. Při vyhodnocení a zpracování obsahu schránky elektronické pošty musí pověřený zaměstnanec dodržet mlčenlivost a ochranu soukromí.

6.2.3. V případě ukončení smluvního ujednání schránka zaniká do 1 měsíce a s ní i veškerý obsah.

7. Bezpečnostní incident

7.1. Základní bezpečnostní incidenty

a) projev počítačového viru nebo jiného zlomyslného SW,

b) nestandardní chování zařízení ICT ČP,

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

d) ztráta nebo odcizení 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.

7.2. Řešení bezpečnostního incidentu

7.2.1. Každý bezpečnostní incident musí uživatel neprodleně oznámit na ServiceDesk ČP.

7.2.2. Uživatel je povinen poskytnout odborným útvarům ČP (odbor bezpečnost ICT, provoz ICT) nezbytnou součinnost. Odbor bezpečnost ICT provede potřebná opatření podle vyhodnocení bezpečnostního incidentu pro uvedení ICT systému ČP do bezpečného stavu.

8. Zvládání mimořádných událostí

8.1. Základní typy mimořádných událostí

8.1.1. Oblast fyzické bezpečnosti

a) oheň, kouř nebo výbuch,

b) záplavy nebo prosakování kapalin,

c) narušení konstrukce budovy,

d) přírodní katastrofa.

8.1.2. 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 mimořádných událostí

8.2.1. V případě vzniku mimořádných událostí, které mohou způsobit narušení činností a dopady na ČP nebo partnera, má každý zaměstnanec ČP nebo smluvní partner povinnost poskytnou nezbytnou součinnost pro jejich zvládání.

8.2.2. Uživatel je povinen postupovat podle směrnice SM-30/2008 Zajištění bezpečnosti a ochrany zdraví při práci a směrnice SM-12/2013 Zajištění požární ochrany.

8.2.3. 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 (zabezpečit záznamová média a zařízení s chráněnými informacemi proti zničení nebo ztrátě).

8.2.4. Uživatel je povinen 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 na ServiceDesk ČP.

8.2.5. V případě závady zařízení ICT závadu neodstraňovat vlastními prostředky, ale závadu nahlásit na ServiceDesk ČP.

9. 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 ze smluvního ujednání se všemi důsledky v podobě upozornění na porušení povinností nebo ukončení smluvního ujednání.

10. Související dokumenty

a) SM-1/2015 Bezpečnostní politika ICT

b) SM-5/2013 Ochrana informací

c) SM-3/2013 Informační systém pro řešení mimořádných událostí

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

e) SM-12/2013 Zajištění požární ochrany

11. Závěrečné ustanovení

Výklad a aktualizaci této příručky zajišťuje ČP (odbor bezpečnosti ICT).