**Příloha č. 9**

**Bezpečnostní příručka ICT Balíkovna Partner**

# Zkratky a pojmy

|  |  |
| --- | --- |
| **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. |
| **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, Skype pro firmy, atd.) |
| **Integrita** | znamená zajištění správnosti a úplnosti informací. |
| **Mobilní zařízení**  | přenosný elektronický přístroj s různým programovým vybavením jako např. mobilní telefon, notebook, netbook, smartbook, PDA, tablet, USB zařízení apod. |
| **Nepříznivá událost** | jakákoliv událost, která vede nebo může vést k narušení bezpečnosti nebo činností ČP.  |
| **SW** | Software je programové vybavení počítače - tedy programy a aplikace v počítači či mobilním zařízení. |
| **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. |

# Povinnosti uživatele

1. Chránit informace ČP v listinné i elektronické podobě, se kterými se dostane do kontaktu při výkonu své činnosti, před případným zneužitím, poškozením, zničením nebo ztrátou.
2. Používat pouze schválené postupy a nástroje (např. certifikáty vydané certifikační autoritou, schválený SW) k elektronické ochraně informací.
3. Chránit zařízení a data ICT ČP před poškozením, zničením, ztrátou nebo zneužitím. Zejména uzamykáním kanceláří a pracovních prostor a vždy při odchodu z pracoviště uzamknutím pracovní plochy zařízení nebo odhlášením ze systému.
4. Používat dostatečně silná hesla podle níže uvedených zásad:
5. heslem nebo jeho součástí nesmí být jméno uživatele nebo jeho blízkých, číslo  průkazu, název organizace, 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.
6. délka hesla musí být dlouhé minimálně 8 znaků, doporučeno je použít délku hesla 12 znaků.
7. heslo nesmí uživatel sdílet s jinou osobou,
8. heslo je doporučeno preventivně měnit 1x za ¼ roku,
9. parametry hesla jsou kontrolovány systémem.
10. 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.
11. 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 ČP a dále se řídit jeho pokyny.
12. 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.
13. Nezasahovat do systémového nastavení jednotlivých zařízení ani neprovádět instalaci nedůvěryhodných programů.
14. Nekopírovat SW ČP na jiný počítač nebo jej předávat jiné osobě.
15. Pracovat se zařízením tak, aby chráněné informace nemohly být odposlechnuty, odpozorovány nebo vyčteny ze zpracovávaných dokumentů a obrazovek zařízení jinou nepovolanou osobou.
16. V případě žádosti operačního systému o restartování zařízení, v co nejkratší době ukončit veškerou činnost a restart provést.
17. Hlásit zjištěné bezpečnostní incidenty (viz kapitola 4.1 této přílohy).
18. Hlásit zjištěné mimořádné události Stálé operační službě na telefonní číslo 605 22 55 55. Jedná se zejména o narušení nebo zničení důležitých zabezpečovacích zařízení, výpadek dodávky elektrické energie spojený s vyřazením elektronických systémů.

# Uživateli je zakázáno

1. Přerušovat probíhající aktualizace systému, vypínat antivirovou ochranu nebo měnit konfiguraci bezpečnostních prvků ochrany.
2. Pracovat s cizími autentizačními nebo přístupovými údaji.
3. Využívat chybně přidělená oprávnění, která mu nepřísluší.

# Bezpečnostní incident

## Základní bezpečnostní incidenty

1. Projev počítačového viru nebo jiného škodlivého SW.
2. Nestandardní chování zařízení nebo uživatelů.
3. Kompromitace nebo zneužití autentizačních a přístupových údajů (např. hesla), podezření nebo pokus o kompromitaci (např. podvodné emaily, neúmyslné prozrazení hesla, apod.).
4. Ztráta nebo odcizení zařízení, mobilního zařízení nebo záznamového média obsahující informace ČP.
5. Proniknutí nepovolané osoby na pracoviště Balíkovny Partner, k zařízení nebo i pokus o nepovolené proniknutí.
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.
9. Chybně přidělená oprávnění nad rámec mu svěřených pracovních povinností.

## Řešení bezpečnostního incidentu

1. Každý bezpečnostní incident nebo podezření na něj musí uživatel neprodleně oznámit na ServiceDesk ČP, případně přes svého nadřízeného, který incident oznámí na ServiceDesk ČP 800 26 00 26.
2. Uživatel je povinen poskytnout ČP nezbytnou součinnost při šetření a řešení bezpečnostního incidentu. Na základě vyhodnocení bezpečnostního incidentu specializovaný útvar ČP provede potřebná opatření pro uvedení systému ČP do bezpečného stavu.

# Doporučené nastavení zařízení Balíkovny Partner

V zájmu zajištění bezpečnosti doporučujeme při provozování systémů ČP používat zařízení, které:

* neobsahuje žádný nelegální SW či SW instalovaný z nedůvěryhodných zdrojů,
* používat výhradně podporovaný a aktualizovaný operační systém,
* používat pouze podporovaný a aktualizovaný Internetový prohlížeč,
* pokud je to možné používat SW pro antivirovou ochranu zařízení.