

Pravidla bezpečného chování uživatele

PO je jako zaměstnavatel, z důvodu zajištění kybernetické bezpečnosti, oprávněn k monitoringu užívání informačních a komunikačních technologií na pracovišti prostřednictvím auditních záznamů používaných místních aplikací, informací o využití elektronické pošty, obsahu zpráv pracovní povahy a statistik navštívených webových stránek zaměstnancem/uživatelé.

Uživatel používající místní aplikace je povinen:

- a) Pro přístup k místním aplikacím používat pouze své přidělené přístupové jméno a heslo.
- b) Při prvním přihlášení k místním aplikacím si musí změnit přidělené heslo.
- c) Zachovávat jedinečnost a důvěrnost přístupového hesla, tj. nikomu heslo nesdělovat (včetně kolegů, Vedoucích zaměstnanců apod.), nikde a nijak jej nezaznamenávat.
- d) Zajistit při zadávání přístupového hesla nemožnost jeho odpozorování druhou osobou.
- e) Při přihlašování k místním aplikacím prostřednictvím webového prohlížeče nevyužívat funkci „zapamatovat heslo“.
- f) Dodržovat pravidla pro tvorbu přístupového hesla k místním aplikacím. Minimální požadavky na heslo jsou:
 - minimální délka hesla: 12 znaků,
 - heslo musí obsahovat alespoň 3 ze 4 skupin znaků (malá písmena, velká písmena, číslice nebo speciální znaky).
- g) Další pravidla pro použití hesel jsou:
 - maximální platnost hesla: 18 měsíců,
 - minimální platnost hesla: 24 hodin,
 - historie hesel: 12 hesla,
 - maximální počet neúspěšných pokusů o přihlášení: 5,
 - doba zablokování účtu po neúspěšných pokusech o přihlášení: 30 minut.
- h) V případě jakéhokoli podezření na kompromitaci hesla nebo jeho zneužití změnit okamžitě heslo a tuto informaci ohlásit Správci ICT.
- i) Před opuštěním pracoviště, i krátkodobém (např. na toaletu), zabezpečit zařízení PO uzamčením pracovní plochy nebo odhlášením se od zařízení PO.
- j) Dodržovat pravidlo „prázdného stolu“, to znamená, že všechny dokumenty obsahující neveřejné informace nebo osobní údaje, které se v danou chvíli nezpracovávají, jsou uloženy v uzamykatelných skříních.
- k) Dodržovat pravidlo „prázdné obrazovky“, to znamená, že všechny otevřené dokumenty na obrazovce zařízení nejsou zpřístupněny neoprávněným osobám.
- l) Neinstalovat žádný software na zařízení PO.
- m) Nestahovat soubory, filmy, hudbu, e-knihy z neautorizovaných stránek.
- n) Nezasahovat do zařízení PO a její konfigurace, vyjma situací, kdy toto bude vyžadováno přímo Správcem ICT.
- o) Řádně zálohovat svá pracovní data dle postupů stanovených Správcem ICT.
- p) Nekopírovat, neukládat, nepřenášet jakákoliv data organizace mimo prostory PO.
- q) Nepoužívat pro výkon pracovní činnosti jakékoliv soukromé či neznámé datové nosiče (např. CD, flash disky, externí HDD).

- r) Nenavštěvovat rizikové internetové stránky a neklikat na reklamní bannery na webu.
- s) Důsledně ověřovat doručenou elektronickou poštu a v případě podezření, že se jedná o závadný e-mail (spam, podvodný e-mail apod.), takovou zprávu neotvírat, nereagovat na ní a tuto skutečnost neprodleně ohlásit Správci ICT nebo Vedoucímu zaměstnanci.
- t) Netisknout data z místních aplikací PO pro jiné než pracovní účely.
- u) V případě zasílání e-mailů s šifrovanou přílohou, předat heslo příjemci jinou cestou (např. telefonicky, SMS apod.). Heslo nikdy nesmí být součástí odesílaného e-mailu. Hesla k jednotlivým souborům se řídí pravidly jako hesla k uživatelským účtům.
- v) Neprodleně hlásit kompromitaci nebo ztrátu jakéhokoliv zařízení či dat zpracovávaných v nesdílených aplikacích správci ICT/Manažerovi kybernetické bezpečnosti a Vedoucímu zaměstnanci.

Kybernetickou bezpečnostní událostí může být mimo jiné:

- a. ponechání přihlášeného zařízení bez dozoru,
- b. zachycení nevyžádaného e-mailu s přílohou (např. výzva k zaplacení faktury),
- c. podezření na kompromitaci přihlašovacích údajů,
- d. nalezení neznámého flash disku apod.

Kybernetickým bezpečnostním incidentem může být mimo jiné:

- a. ztráta zařízení (notebook, flash disk, smartphone apod.),
- b. zjištění použití hesla jinou osobou,
- c. napadení škodlivým SW,
- d. narušení fyzické bezpečnosti organizace/kanceláře,
- e. předání přihlašovacích údajů jiné osobě (včetně kolegů či vedoucích) apod.

Výše uvedená pravidla jsou závazná pro jakoukoliv činnost s informacemi PO, prováděnou na pracovních stanicích, přenosných a částečně i na soukromých zařízeních, využívaných pro pracovní účely.

Použití přístupového hesla

Heslo nesmí obsahovat jméno uživatelského účtu nebo části jména a příjmení uživatele.

Je zakázáno používání známých jmen, osobních údajů a jiných lehce odhalitelných hesel (jako jsou datum narození, jména členů rodiny, názvy předmětů v blízkosti počítače, běžných jednoduchých slov umožňujících tzv. slovníkový útok, apod.).

Hesla je nutno udržovat v tajnosti, tj. nikomu je nesdělovat ani nezapisovat na lehce přístupná místa (zápisník, okraj monitoru, kalendář apod.).

Pravidla pro ochranu a používání přenosných zařízení

Ochrana přenosných zařízení:

Zaměstnanci mají povoleno vykonávat pracovní činnost mimo objekty PO pouze po schválení Vedoucím zaměstnancem.

Za ochranu přiděleného přenosného zařízení PO je vždy odpovědný zaměstnanec.

Ochrana soukromých zařízení:

Zaměstnanec bere na vědomí, že převzetím přístupových oprávnění k místním aplikacím přebírá odpovědnost za zajištění minimální úrovně ochrany soukromých zařízení, kterou je povinen při přístupu k místním aplikacím zajistit.

Soukromá zařízení, jejímž prostřednictvím zaměstnanec přistupuje k místním aplikacím, musí být:

- a) Vybavena pravidelně aktualizovaným operačním systémem.
- b) Vybavena pravidelně aktualizovanou antivirovou aplikací.
- c) Chráněna za pomoci přihlašovacích údajů uživatele, s:
 - minimální délkou hesla: 8 znaků, a
 - použití alespoň 3 ze 4 skupin znaků (malá písmena, velká písmena, číslice nebo speciální znaky).
- d) Nastavena tak, aby se po 5 minutách neaktivity uživatele uzamkla, v případě smartphonu a tabletu po 2 minutách neaktivity.
- e) Smartphony a tablety chráněny PINem, biometrickým údajem nebo heslem s alespoň 6 znaky.
- f) Vybaveny pouze aplikacemi instalovanými z oficiálních obchodů (např. Google Play, Apple store, Galaxy store apod.).

Pravidla pro používání přenosných a soukromých zařízení

Při používání přenosných a soukromých zařízení pro připojení k místním aplikacím jsou zaměstnanci povinni:

- a) Učinit všechna dostupná opatření, která mohou zabránit ztrátě či odcizení zařízení (neponechávají je bez dohledu a/nebo zabezpečení např. v dopravních prostředcích, v ubytovacích zařízeních apod.).
- b) Pro připojení k internetu prostřednictvím WI-FI sítě využívat pouze šifrovaného, zabezpečeného připojení (připojení prostřednictvím hesla, důvěryhodný poskytovatel – úřad, pořadatel školení apod.) a po ukončení práce se odpojit od místních aplikací (zásadně nelze využívat např. free WI-Fi v nákupních centrech, hotelích, nádražích apod.).

- c) Aktivně zabraňovat odpozorování obrazovky cizí osobou (např. ve vlacích, restauracích, na lavičkách, v prostředcích hromadné dopravy apod.).
- d) Neumožnit přístup ke zpracovávaným informacím v místních aplikacích jiné osobě, včetně rodinných příslušníků.

Pravidla bezpečného používání zařízení

Zařízení PO, jejich prostřednictvím je možné přistupovat k místním aplikacím, musí být minimálně:

- a) vybavena pravidelně aktualizovaným operačním systémem,
- b) vybavena pravidelně aktualizovanou antivirovou aplikací,
- c) chráněna za pomoci přihlašovacích údajů uživatele (viz kap. „Pravidla bezpečného chování uživatele“),
- d) nastavena tak, aby se po 10 minutách neaktivity uživatele uzamkla, v případě smartphonu a tabletu po 2 minutách neaktivity,
- e) nastavena tak, aby uživatel disponoval pouze účtem s oprávněním „standardní uživatel“,
- f) smartphony a tablety chráněny PINem, biometrickým údajem nebo heslem s alespoň 6 znaky,
- g) vybaveny pouze schválenými aplikacemi,
- h) u přenosných zařízení pevný disk šifrován, pokud to operační systém umožňuje,
- i) vyměnitelné médium (např. USB disk, externí pevný disk apod.) připojené k pracovní stanici nebo přenosnému zařízení, zkontrolováno antivirovým SW,
- j) vyměnitelné médium šifrováno, v případě ukládání dat z místních aplikací.

Správce ICT odpovídá za nastavení zařízení připojujících se k místním aplikacím dle pravidel uvedených výše.

Manažer kybernetické bezpečnosti ve spolupráci se Správcem ICT stanovuje pravidla pro centralizovanou správu zařízení, včetně přenosných zařízení, prostřednictvím např. AD, MDM apod.

Kybernetické bezpečnostní incidenty

Zaměstnanci jsou povinni, v případě zjištění kybernetické bezpečnostní události/incidentu, neprodleně informovat Správce ICT, Manažera kybernetické bezpečnosti nebo ředitele PO (viz také kap. Bezpečné chování uživatele).

PO následně zavede nápravná opatření a vyhodnocuje jejich účinnost a následně seznámí zaměstnance s kybernetickým bezpečnostním incidentem a jeho příčinami.