Směrnice č. 14/2019 - 02

Pravidla systémů informačních technologií (IT)

FEDERACE ŽIDOVSKÝCH OBCÍ V ČR

Účelem tohoto předpisu je úprava pravidel provozu informačních technologií, pravidel chování uživatelů při jejich využívání, tedy využívání technického a programového vybavení Federace židovských obcí v ČR (dále jen FŽO) a dále pravidel pro elektronickou komunikaci.

Článek 1
Úvodní ustanovení

(1) Tato směrnice stanovuje pravidla provozu počítačové sítě (dále jen „počítačová síť"), chování jejích uživatelů a používání technického a programového vybavení v rámci FŽO.

(2) Směrnice dále stanovuje pravidla uživatelské a technické podpory, komunikace a řešení incidentů v počítačové síti FŽO.

Článek 2
Základní pojmy

Pro účely této směrnice se rozumí:

a) **pověřený správce informačních technologií (dále jen správce IT)** – externí dodavatel, který spravuje informační systémy a technologie FŽO na základě smlouvy.

b) **programové vybavení (software)** - sada všech počítačových programů používaných v počítači, které provádějí nějakou činnost,

c) **technické vybavení (hardware**) – souhrn technických prostředků výpočetní a komunikační techniky, zejména počítače a jejich komponenty, periferie (tiskárny, monitory apod.) včetně jejich komponent a prvky datových sítí včetně jejich komponent, mobilní zařízení.

d) **licenční smlouva a licenční ujednání** – právní dokument, kterým autor poskytuje nabyvateli oprávnění k výkonu práva užít programového vybavení stanoveným způsobem a ve stanoveném rozsahu,

e) **počítačová síť'** FŽO - soubor všech technických prostředků (hardware + software), evidovaných v rámci majetkové či jiné evidence FŽO, umožňující všem připojeným počítačům jejich vzájemnou komunikaci a současně zajišťující dostupnost nebo sdílení společných informačních zdrojů a služeb (např. internet).

f) **IS** – informační systémy FŽO,

g) uživatel počítačové sítě FŽO (dále jen „uživatel) je:

   i) zaměstnanec FŽO v pracovním poměru, který má zřízen uživatelský účet v počítačové síti,

ii) pracovník s dohodou o provedení práce nebo dohodou o pracovní činnosti, který má zřízen uživatelský účet v počítačové síti FŽO,

h) **uživatelský účet** – je soubor informací v počítačové síti FŽO, vytvořený pověřeným správcem sítě pro každého uživatele, který jej při přístupu do počítačové sítě FŽO jednoznačně určuje včetně jeho pracovního prostředí,

i) **uživatelské jméno / doménový login** – unikátní řetězec znaků, sloužící společně s heslem k identifikaci a ověření (autentizaci) uživatele při přístupu do počítačové sítě FŽO a dalšího programového vybavení v rámci IS,

j) **heslo** – bezpečnostní opatření, které zpřístupňuje dané prostředky pouze osobě, která toto heslo zná. Princip ochrany heslem spočívá ve spřažení uživatelského jména oprávněné osoby s řetězcem znaků – vlastním heslem.

k) **identifikace uživatele** – proces určení identity uživatele. Identitu udává uživatel a identifikující systém se snaží určit identitu uživatele v předem dané databázi uživatelských záznamů (např. uživatelské jméno a heslo), tedy provést autentizaci uživatele,

l) **autentizace uživatele** – proces ověření (verifikace) proklamované identity uživatele. Po dokončení autentizace následuje proces autorizace, tj. přiřazení oprávnění (na základě identity uživatele a příslušné bezpečnostní politiky) pro práci v systému a specifikace co daný uživatel může, příp. nemůže,

m) **autorizace uživatele** - proces zajišťující přidělení přístupových práv uživatele k objektu(ům) nebo k provedení konkrétní operace, tedy právo uživatele definovaným způsobem pracovat s určitými daty nebo používat IS,

n) **autorizovaný uživatel** - uživatel, který má přístupové právo nebo povolení pracovat v IS a s aplikacemi podle předem stanovených zásad přístupu,

o) **pracovní (uživatelská) stanice** – stolní osobní počítač nebo notebook včetně nezbytných periferií,

p) **server** – speciální počítač v počítačové sítí FŽO, poskytující služby uživatelům,

q) **mobilní zařízení** – technické zařízení, které umožňuje činnost zaměstnance mimo prostory FŽO, je dostatečně malé a umožňuje práci v pohybu, nebo může být přemísťováno, např. notebooky, "chytré" telefony, tablety, digitální fotoaparáty, přenosné disky atd,

r) **technická podpora** – služba správce informačních systémů, jejímž cílem je poskytování technické a metodické podpory uživatelům v počítačové síti FŽO,

s) **Osobní údaj** - Jakýkoliv údaj, který se týká přímo či nepřímo identifikovatelné osoby. Nejedná se tedy pouze o údaje, na základě kterých je možné člověka identifikovat, ale veškeré údaje, které se této osoby týkají (včetně IP adres či obrázků obličejů).

t) **Zvláštní kategorie os. údajů –** osobní údaj, který vypovídá o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, genetické a biometrické údaje zpracovávané za účelem jedinečné identifikace fyzické osoby, údaje o zdravotním stavu, sexuálním životě nebo sexuální orientaci fyzické osoby.

u) **Internet** - komplexní globální síť skládající se z tisíce dalších nezávislých sítí, které jsou provozované vládními agenturami, výchovně-vzdělávacími a výzkumnými institucemi a soukromými obchodními společnostmi. Slouží jako přenosové médium pro různé informace a služby (např. elektronická pošta, systém vzájemně propojených stránek a dokumentů WWW apod.).

Článek 3
Základní povinnosti uživatele

(1) Uživatel se musí chovat tak, aby neporušoval platný právní řád České republiky a zejména interní předpisy FŽO.

(2) Uživatel je povinen zejména:

a) hlásit bez prodlení svému nadřízenému nebo správci IT jakékoliv podezření na porušení této směrnice, závadné chování jiných uživatelů (např. zneužití přístupu do sítě, podezření na nelegální činnost, odcizení či zneužití dat), závady technického nebo programového vybavení, podezření na nelegální programové vybavení nebo podezření na incident z oblasti kybernetické bezpečnosti,

b) využívat počítačovou síť FŽO pouze pro pracovní činnosti, související s jeho pracovní náplní,

c) užívat k práci na pracovní stanici nebo notebooku pouze legální programové vybavení, které je určeno pro jeho práci nebo studium a instalováno správcem IT nebo s jejich souhlasem,

d) postupovat tak, aby jeho činnost v co nejmenším rozsahu negativně ovlivňovala možnosti využití prostředků počítačové sítě FŽO dalšími uživateli (např. neúměrným zatěžováním datových linek, neúměrným zatěžováním serverů apod.). V případě, že je v rámci plnění jeho pracovních úkolů nezbytné využit prostředků počítačové sítě FŽO nad obvyklý rámec, konzultuje způsob provedení úkolu se správcem IT a řídí se dále jejich pokyny.

e) zajistit dostatečnou softwarovou a fyzickou ochranu pracovních dat v případě pracovní nutnosti mít v souladu s podmínkami této směrnice (čl. 3, odst. 3, písm. f této směrnice) pracovní data na přenosném zařízení nebo paměti.

(3) Uživatel nesmí zejména:

a) využívat prostředky počítačové sítě FŽO k soukromým, komerčním nebo jiným účelům nesouvisejícím s jeho pracovní náplní,

b) umožnit přístup k počítačové síti FŽO fyzickým či právnickým osobám, které nejsou uživateli,

c) instalovat na počítač programy umožňující vzdálené ovládání počítače z internetu (např. programy Teamviewer, LogMeIn, VNC apod.),

d) jakýmkoli způsobem poškozovat prostředky počítačové sítě FŽO ani je vystavovat jakémukoliv nebezpečí,

e) bez souhlasu nebo pokynu zaměstnavatele pořizovat jakékoli kopie programového vybavení instalovaného na prostředcích FŽO, na prostředky, které nejsou v majetku FŽO, a to ať již pro potřebu svou nebo osoby cizí,

f) bez souhlasu nebo pokynu zaměstnavatele pořizovat kopie jakýchkoliv pracovních dat z počítače nebo z počítačové sítě na přenosná paměťová média (např. USB flash disky nebo externí pevné disky) nebo na přenosná zařízení (např. notebooky, telefony), který zváží, zda je to nutné z důvodu pracovních povinností,

g) bez souhlasu nebo pokynu zaměstnavatele pořizovat jakékoliv exporty, copy&paste kopie, printscreeny, tisky z uživatelských rozhraní interních systémů, softwarů, databází a i webových aplikací obsahující osobní údaje nebo zvláštní kategorie osobních údajů,

h) bez souhlasu nebo pokynu zaměstnavatele poskytovat, předávat nebo sdílet jakoukoliv formou jakákoliv pracovní data třetí osobě v nepracovním poměru s FŽO nebo osobě bez oprávnění přístupu k těmto předávaným datům,

i) bez souhlasu nebo pokynu zaměstnavatele instalovat na počítač programy umožňující přístupy ke cloudovým službám (např. Google Drive, One Drive, Drop Box apod.) a následně jich využívat pro ukládání pracovních dat z počítače nebo počítačové sítě,

j) instalovat na počítač obecně jakýkoliv program nesouvisející s pracovními povinnostmi a bez souhlasu správce sítě,

k) ukládat na prostředky počítačové sítě FŽO multimediální soubory a instalační soubory programů, na které se vztahuje autorský zákon a jež nejsou v majetkové evidenci FŽO nebo na něž FŽO nevlastní licenční práva,

l) odstraňovat informace nebo označení identifikující autorská práva k programovému vybavení,

m) pracovat pod cizí identitou, používat prostředky k jejímu získání nebo zneužít v tomto pochybení či nedbalosti jiného uživatele,

n) sledovat nebo odposlouchávat provoz na počítačové síti FŽO. O výjimce z tohoto pravidla rozhoduje tajemník FŽO,

o) provádět výměny, stěhování, čištění, odpojení či připojování zařízení k počítačové síti FŽO, opravy a změny konfigurace technického a programového vybavení nad rámec jeho uživatelských práv s výjimkou přemisťování mobilních zařízení, předaných uživateli do užívání,

p) připojovat jakékoliv hardwarové zařízení na počítačovou síť (např. vlastní síťové disky, wifi routery apod.) bez souhlasu správce sítě (možná výjimka je připojení pracovních mobilních telefonů nebo notebooků k bezdrátové wifi síti FŽO),

q) připojovat jakékoliv hardwarové zařízení k počítači bez souhlasu správce sítě.

Článek 4
Uživatelský účet a přístupová oprávnění

(1) Přístup k počítačové síti FŽO je podmíněn jednoznačnou identifikací každého uživatele (tzv. identita uživatele), tj. přihlášením k jeho uživatelskému účtu (dále jen „účet“). Přístup uživatele k počítačové síti je tak možný pouze autentizovaně pomocí uživatelského jména a hesla. Uživatelské jméno je vždy unikátní, stanovené uživatelem. Heslo si uživatel vždy volí sám dle příslušných pravidel (viz níže bod 3).

(2) S každým jednotlivým účtem jsou spojena určitá přístupová práva, která určují oprávnění uživatele ve vztahu ke zdrojům a službám počítačové sítě FŽO.

(3) Uživatel, kterému je účet zřízen, je povinen jej chránit heslem, jehož struktura musí splňovat následující požadavky:

i) Heslo má min. 8 znaků,
ii) Heslo obsahuje **velká a malá písmena a čísla,**
iii) Heslo se liší od uživatelského jména.

Účet může být chráněn rovněž biometrickým údajem.

(4) Heslo je zaměstnanec povinen udržovat v tajnosti. Heslo ke svému účtu nesmí sdělit druhé osobě. Heslo také nesmí být zasíláno nezabezpečenou elektronickou poštou.

(5) Uživatel je oprávněn provádět změnu hesla.

(6) Za určitých podmínek je uživatel povinen heslo změnit (např. v případě podezření jeho prozrazení neoprávněné osobě). V rámci příslušné bezpečnostní politiky může být také vynucován požadavek na pravidelnou změnu hesla.

(7) V rámci provozu IS může být u některých síťových aplikací vyžadována dodatečná autentizace uživatele. Do těchto aplikací se mohou přihlásit jen uživatelé, kteří mají přiřazeny administrátorem příslušné role. Tyto role jim následně umožnují přístup do částí aplikace, které potřebují k vykonávání svých pracovních povinností.

(8) Uživatel smí používat pouze ta přístupová práva, která mu řádným způsobem náleží, a nesmí vyvíjet žádnou činnost směřující k obejití tohoto ustanovení. Pokud uživatel jakýmkoliv způsobem získá přístupová práva, která mu nebyla přidělena (např. chybou programů nebo technického vybavení), je povinen tuto skutečnost neprodleně oznámit správci IT. Takto získaná práva nesmí použít. Uživatel nesmí zneužít nedbalosti jiného uživatele (např. opomenuté odhlášení) k tomu, aby v počítačové síti FŽO pracoval pod cizí identitou.

(9) V případě skončení pracovního poměru zaměstnance zabezpečí přímý nadřízený zaměstnance v součinnosti se správcem IT deaktivaci účtu zaměstnance. Případné výjimky z tohoto pravidla povoluje tajemník FŽO.

(10) Tajemník FŽO nebo pověřený vedoucí zaměstnanec FŽO má v odůvodněných případech právo vydat pokyn k dočasnému zablokování přístupu k počítačové síti FŽO uživateli, který hrubým způsobem porušil (nebo trvale porušuje) ustanovení této směrnice.

Článek 5
Základní pravidla užívání počítačové sítě FŽO

(1) Uživatel využívá svěřené počítačové prostředky, kopírovací a tiskové služby, ve shodě se svými pracovními úkoly.

(2) Pracovní stanice uživatelů jsou prostřednictvím počítačové sítě standardně připojeny do Internetu. Případné výjimky o nepřipojení pracovní stanice (např. z důvodu bezpečnosti) může rozhodnout tajemník FŽO nebo pověřený vedoucí zaměstnanec FŽO.

(3) Zaměstnanec může být vybaven mobilním zařízením. Zařízení, výběr poskytovatele mobilního připojení a příslušný tarif schvaluje vedoucí střediska pověřené gescí za IT.

(4) Odpovědnost za připojovaná mobilní zařízení nese vždy uživatel. Odpovídá především za zabezpečení svého zařízení, tedy i antivirovou ochranu a instalovaný software. V případě zjištění problému s výše uvedenými body, je správce IT FŽO oprávněn zařízení uživatele odpojit.

(5) FŽO může bezplatně poskytnout zaměstnancům software, který ze svého licenčního ujednání lze použít i pro domácí použití na zařízení patřícím uživateli.

(6) Provoz počítačové sítě FŽO, aplikací a přístupu uživatelů k nim může být monitorován. Monitoring provádí určený dodavatel s příslušným smluvním vztahem s FŽO.

Článek 6
Provoz základních síťových služeb

V rámci provozu počítačové sítě FŽO je, kromě jiných, zajišťován provoz těchto základních služeb.

1) Elektronická pošta:

a) poštovní schránka (e-mail) je zřizována na základě žádosti příslušného nadřízeného,

b) Zaměstnanec je povinen při komunikaci s ostatními zaměstnanci FŽO, s klienty a obchodními partnery používat e-mailové adresy zřízené zaměstnavatelem. Porušení tohoto pravidla je považováno za porušení pracovních povinností.

c) velikost přílohy odesílaného e-mailu je systémově omezena a při jejím překročení nebude odeslání uživateli e-mailu umožněno,

d) systémově je zamezeno přijímat nebo odesílat přílohy, obsahující soubory umožňující spustit škodlivý kód,

e) v souvislosti s ukončením pracovního poměru zaměstnance, dojde ke zrušení e-mailové schránky uživatele po uplynutí 3 měsíců od data ukončení, pokud vedoucí příslušného útvaru v požadavku zaslaném e-mailem na adresu správce IT nestanovil delší dobu.

2) Sdílené síťové úložiště:

a) každý uživatel má při zřízení účtu automaticky přidělen přístup na sdílené síťové diskové úložiště na základě jeho pracovního zařazení. Přístup do některých sekcí sdíleného úložiště může být omezen na základě rozhodnutí vedoucího střediska uživatele.

b) přístupová oprávnění uživatele musí být definována jako vazba na pracovní pozici zaměstnance. Potřebná přístupová oprávnění vždy definuje příslušný nadřízený zaměstnance, u vedoucích zaměstnanců oprávnění definuje tajemník FŽO.

c) v případě změny pracovní pozice musí být odpovídajícím způsobem změněna i přístupová oprávnění uživatelského účtu zaměstnance. V případě řadových zaměstnanců zodpovídá za vystavení změnového požadavku příslušný nadřízený, u vedoucích zaměstnanců je zodpovědnou osobou tajemník FŽO.

3) Zálohování dat:

a) Zálohování dat vybraných uživatelských stanic a všech sdílených síťových úložišť je zajišťováno centrálně s výjimkou osobních (vlastních) dat zaměstnanců FŽO, které si zálohují zaměstnanci sami.

b) Centrální zálohování zajišťuje pravidelné zálohy síťového úložiště následujícím způsobem:

i) 1x za 24 hodin je sdílené úložiště zálohováno na oddělený zálohovací síťový disk. Zálohy starší 60ti dnů se cyklicky přepisují.

ii) Správce IT vytvoří 1x za 3 měsíce zálohu na odpojitelný pevný disk, který předá pověřenému zaměstnanci FŽO k bezpečnému uložení do trezoru FŽO výměnou za předchozí uložený disk z trezoru se starou zálohou k příštímu nahrání nové zálohy.

Článek 7
Základní provozní bezpečnostní opatření a ochrana dat

(1) Uživatel je oprávněn využívat k práci pouze počítač, který byl k jeho práci určen.

(2) Přístup uživatele do počítačové sítě FŽO přes počítač přidělený jinému zaměstnanci je možný pouze jen s jeho svolením anebo svolením příslušného nadřízeného, a to vždy pouze jen pod vlastní identitou. Zaměstnanec tedy smí umožnit přístup na jemu přidělený počítač pouze uživatelům, kteří mají platný účet v počítačové síti FŽO.

(3) Při opuštění pracoviště učiní uživatel nezbytná opatření k zabránění zneužití přístupu k datům, a to některou z možností danou operačním systémem dle potřeby (uzamknutí pracovní stanice nebo její vypnutí) a dále zabezpečí pracoviště před vstupem neoprávněné osoby.

(4) Při práci s elektronickou poštou a službami poskytovanými v rámci sítě Internet je uživatel povinen chovat se obezřetně a dodržovat obecná pravidla bezpečnosti ve stanoveném rozsahu. Bezpečnostní pravidla pro práci s elektronickou poštou a Internetem jsou součástí **Bezpečnostní příručky uživatele**.

(5) V případě, že uživatel na své pracovní stanici zaregistruje nestandardní stavy, které svým charakterem zjevně neodpovídají běžnému chování počítače, měl by o tomto neprodleně informovat svého nadřízeného a správce IT.

(6) Vzdálený přístup do počítačové sítě FŽO prostřednictvím sítě Internet není zaměstnancům umožněn. Výjimku může udělit vedoucí střediska pověřené gescí za IT, se souhlasem tajemníka FŽO.

(7) Metodické řízení antivirové ochrany a dalších prvků zabezpečení počítačové sítě FŽO vykonává správce IT.

(8) Přílohy e-mailu, obsahující škodlivý kód, který byl rozpoznán antivirovými nástroji na poštovním serveru, a přílohy ve formě souborů, které jsou potenciálně spustitelné a představují riziko počítačového viru šířeného na běžně používaných platformách, nebudou adresátům doručovány, ale budou neprodleně odstraněny, nebo přesunuty do karantény na serveru.

(9) Při připojení jakéhokoliv datového nosiče k pracovní stanici je zaměstnanec FŽO povinen jej zkontrolovat nainstalovaným antivirovým programem. V případě zjištění problému postupuje zaměstnanec dle instrukcí antivirového programu, neví-li si rady, obrátí se na správce IT.

Článek 8
Nakládání s daty

(1) Uživatelé jsou povinni při nakládání s daty, tzn. při jejich pořizování, zpracovávání, archivaci a šíření, dodržovat obecně závazné právní předpisy České republiky a interní předpisy FŽO.

(2) Data pořízená zaměstnanci FŽO v rámci výkonu jejich pracovní činnosti jsou majetkem FŽO. Zaměstnanec je povinen ukládat data způsobem, který umožní jejich využití ostatními zaměstnanci FŽO. Poskytnutí těchto dat třetím osobám bez souhlasu nadřízeného zaměstnance nebo tajemníka FŽO je považováno za hrubé porušení pracovní kázně.

(3) Pořizování a nakládání s databázemi, datovými sadami či jinými celistvými datovými strukturami od třetích osob, které nejsou volně šiřitelné, musí být vždy podloženo smluvním ujednáním s poskytovatelem těchto dat. Smluvní ujednání musí obsahovat zejména podmínky a způsob, jak je společnost oprávněna s daty nakládat, včetně možnosti a rozsahu jejich dalšího šíření. Nestanoví-li obecné závazné právní předpisy jinak, musí být

tyto podmínky sjednány v písemné smlouvě. Smluvní ujednání musí být vždy schváleno vedoucím střediska pověřeným gescí za IT.

(4) Není-li si uživatel jist jakýmkoliv aspektem pořizování, zpracovávání, archivaci a šíření dat, je povinen konzultovat problematiku se svým nadřízeným.

Článek 9
Soukromí dat uživatelů

(1) FŽO se snaží chránit práva a oprávněné zájmy všech uživatelů své počítačové sítě a v této souvislosti i chránit data a informace uložené na jejich počítačích nebo přenášených počítačovou sítí FŽO. FŽO však nemůže technicky zabezpečit úplné soukromí a bezpečnost uložených nebo přenášených dat. Vysoce citlivá data proto nemohou být na počítačích, připojených do počítačové sítě FŽO, uložena či sítí přenášena bez použití dodatečných prostředků pro jejich zabezpečení, a to minimálně na úrovni šifrování.

(2) Pro zajištění maximální možné míry soukromí a bezpečnosti dat je uživatelům zakázáno:

a) provádění jakýchkoliv akcí vedoucích k neoprávněnému narušení soukromí jiného uživatele, a to i v těch případech, kdy uživatel svá vlastní data explicitně nechrání,

b) prohlížení obsahu uživatelských adresářů, jakož i kopírování jakýchkoliv dat nebo programů z nich bez výslovného svolení uživatele. Toto omezení platí i v případě, že uživatelské adresáře jsou svými oprávněnými uživateli ponechány volně přístupné elektronickými prostředky,

c) odposlouchávání provozu a vytváření kopií zpráv procházejících jednotlivými uzly počítačové sítě FŽO,

d) vědomé využívání neoprávněně získaných dat, případně jejich nabízení jiným subjektům.

Článek 10
Zpracování osobních údajů

(1) Osobní údaje zaměstnanců jsou zpracovávány pouze na pracovní stanici zaměstnance pověřeného vedením personální agendy. Zálohování osobních dat zaměstnanců je prováděno na oddělený zálohovací síťový disk mimo dosah ostatních uživatelů.

(2) Pracovní stanice pověřeného zaměstnance se musí nacházet v samostatně uzamykatelné místnosti, do níž má přístup pouze pověřený zaměstnanec.

(3) Vzájemné zastoupení zaměstnanců při nakládání s osobními údaji je možné pouze na základě rozhodnutí vedoucího pověřeného zaměstnance.

(4) Zaměstnanci nejsou oprávněni vynášet fyzické nosiče osobních údajů mimo prostory zaměstnavatele v rámci sjednaného místa výkonu práce.

Článek 11
Vlastnická a autorská práva

(1) Uživatelé jsou povinni respektovat vlastnická a autorská práva FŽO, ostatních uživatelů i jiných subjektů.

(2) Především je zakázáno:

a) poškozování, zcizování nebo ničení počítačů, programového vybavení, komunikačních linek, či jiných počítačových prostředků,

b) neautorizovaná modifikace programů, dat nebo technického vybavení. Obzvláště nesmějí být prováděny neautorizované změny konfigurace počítačových prostředků, které by mohly mít vliv na provoz celé sítě,

c) neoprávněná instalace, sdělování veřejnosti nebo rozmnožování počítačových programů, databází a dalších výsledků tvůrčí duševní činnosti, které jsou chráněny autorským zákonem, neautorizované kopírování, byť i částí, dat,

d) užívání počítačové sítě k získání neautorizovaného přístupu k neveřejným informačním zdrojům.

Článek 12
Správce sítě (IT)

Pověřený správce sítě je oprávněn k přístupu ke všem pevným pracovním stanicím a notebookům ve vlastnictví FŽO a k datům na nich uloženým. Musí však přitom dbát, aby jeho počínání bylo v souladu s obecně platnými předpisy, zejména s nařízením GDPR.

Článek 13
Uživatelská podpora uživatelů, komunikace a řešení incidentů

(1) Uživatelskou a metodickou podporu uživatelů provádí pověřený správce IT FŽO .

(2) V případě problému se zaměstnanec obrátí na vedoucího střediska FŽO pověřeného gescí za IT, který problém komunikuje s pověřeným správcem IT FŽO.

Článek 14
Porušení pravidel a sankce

(1) Porušení ustanovení této směrnice může být u zaměstnanců považováno za porušení základních povinností zaměstnance[1] a lze z něj vyvodit příslušné pracovněprávní důsledky včetně rozvázání pracovního poměru.

(2) Porušení pravidel stanovených touto směrnicí, případně dalších obecně závazných právních předpisů v oblasti IS, se posuzuje vždy především s ohledem na závažnost tohoto porušení.

(3) Porušení povinností stanovených v odst. (6) - (8) článku 10 je **hrubým porušením pracovních povinností** a může být důvodem k okamžitému rozvázání pracovního poměru.

(4) Při jakémkoliv zjištění závažného porušení pravidel ze strany uživatelů, v jehož důsledku hrozí možnost následného vzniku dalších škod, musí být vždy nejprve zajištěna náprava, a to takovým způsobem (pokud možno), aby bylo dalším škodám zabráněno.

[1] § 301 , písm. b) až d) zákona č. 262/2006 Sb., zákoníku práce

Článek 15
Závěrečná ustanovení

(1) Tato směrnice vstupuje v platnost dnem 26. 6. 2019.

……..

Ing. Petr Papoušek, předseda

Příloha: Bezpečnostní příručka

Příloha ke směrnici č. 14/2019 - 02

Federace židovských obcí v ČR

Bezpečnostní příručka uživatele

Následující výčty nebezpečných typů souborů se týkají jak příloh emailů, tak i jakýchkoliv souborů stažitelných z internetu, tak i přinesených na přenosných paměťových nosičích nebo zařízeních.

1) Nebezpečné přípony souborů

V žádném případě neotvírat a spouštět soubory končící příponou ade, adp, app, asd, asf, asx, bas, bat, bta, chm, cmd, com, cpl, crt, dll, exe, fxp, hlp, hta, hto, inf, ini, ins, isp, ,js, jse, lib, lnk, mdb, mde, msc, msi, msp, mst, obj, ocx, ovl, pcd, pif, prg, reg, scr, sct, sh, shb, shs, sys, url, vb, vba, vbe, vbs, vcs, vxd, wmd, wms, wmz, wsc, wsf, wsh atd. Jedná se o soubory, které jsou přímo nebo nepřímo spustitelné. Takové emaily rovnou mazat. Jedinou výjimkou jsou situace, kdy soubor s potenciálně nebezpečnou příponou očekáváte.

Většina mailových poskytovatelů tyto soubory blokuje přímo na serveru. Proto je útočníci balí do archívů (zip, rar, 7z, atd.), aby tyto infikované přílohy prošly prvním, hrubým sítem na serveru.

2) Soubory s relativně bezpečnou příponou

Viry a trojské koně často využívají trik s dvojí příponou. Při výchozím nastavení OS Windows schovává známou příponu souboru. Díky tomu se infikovaný soubor zobrazuje jako by měl bezpečnou příponu. Například obrazek.jpg.exe se zobrazí jako obrazek.jpg. Proto je potřeba si dát pozor na tyto soubory s dvojitou příponou např. nazev-dokumentu.doc.exe nebo faktura.pdf.exe. **NEOTEVÍRAT**!

3) Opatrnost i u relativně bezpečných příloh

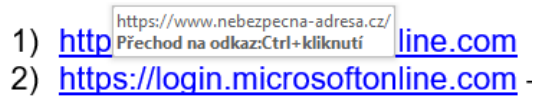
S rozmyslem otevírat přílohy s příponami typu , *.doc, *.docx, *.xls, *.xlsx, *.ppt, *.pptx, *.html, *.htm, atd. které můžou obsahovat škodlivý ActiveX script nebo makro. Tady je potřeba použít zdravý rozum a rozumný odhad. Pokud si nejste jistí, jestli je příloha v pořádku, je nutné se obrátit na správce sítě.

4) Opatrnost při klikání na internetové odkazy, zejména v mailech

Velmi častým způsobem, jak útočníci oklamávají uživatele, je předstírání věrohodné internetové adresy v odkazu, i když skutečný odkaz vede na nebezpečné místo. Vlastností internetových odkazů v jazyku html, kterým jsou tvořeny internetové stránky i emaily, je to, že internetový odkaz se může jmenovat libovolně a název se nemusí shodovat se skutečnou URL adresou odkazu. Proto následující zdánlivě stejně vypadající odkazy jsou naprosto odlišné:

1) https://login.microsoftonline.com - skutečně vede na přihlašovací stránku Microsoftu
2) https://login.microsoftonline.com – vede na smyšlenou nebezpečnou stránku.

Nesmíte nikdy věřit, že odkaz vede tam, jak vypadá. Např. u podezřelých emailů vyzývajících vás k nějaké akci na uvedeném odkazu si vždy musíte zkontrolovat, zda se skutečně odkazovaná URL adresa shoduje s názvem odkazu. Typicky toto lze ověřit najetím kurzoru myši nad odkaz, kdy se zobrazí „bublina“ se skutečně odkazovanou URL adresou.



Ukázka kontroly odkazu najetím kurzoru myši nad něj

5) Rozpoznání podvržené stránky, která od vás chce vyplnit citlivé údaje (phishing)

Pokud jste na webové stránce, do které zadáváte citlivé údaje jako např. přihlašovací informace jako jméno a heslo nebo číslo platební karty, vždy se ujistěte, že URL adresa uvedená v URL řádku stránky se shoduje s vaším očekáváním. Tato opatrnost je zejména na místě, pokud na takovou webovou stránku jste se dostali kliknutím na odkaz uvedeném v pochybném emailu nebo webové stránce. Útočníci velmi často předstírají cizí identitu včetně dokonalé kopie vzhledu stránky a uživatel si domnívá, že se nachází na přihlašovací stránce např. banky nebo platební brány.

6) Napadení vyděračským softwarem – Ransomware

Jedná se o rozšířené a velmi nebezpečné napadení počítače škodlivým programem, který zpravidla šifruje data v něm zapsaná, ale i mimo něj v počítačové síti a požadující od uživatele výkupné za obnovení přístupu k datům. Pokud přes veškerou opatrnost výše uvedenou uživatel spustí program, obsahující ransomware, existují příznaky, jak poznat nákazu:

- počítač se razantně zpomalí vlivem zátěže způsobené šifrováním souborů
- soubory obsahující uživatelská data (typicky dokumenty) začnou měnit své názvy a koncovky a zdvojí se. První soubor obsahuje šifrovaný obsah původního souboru, druhý pak obsahuje textovou informaci obsahující informaci pro uživatele, co se stalo s daty a co má udělat k tomu, aby se k datům dostal.

Pokud zpozorujete zejména druhý uvedený příznak, okamžitě vypněte počítač a odpojte ho od počítačové sítě a kontaktuje správce IT.