Směrnice „Bezpečnost ICT“

Vypracoval:	Martin Píša, Michal Nosek	Vydáno dne: 25.5.2019
Schválil: ředitel školy	Mgr. Bohumil Herčík	Účinnost od: 25.5.2019
ČJ.	265/19	Nahrazuje

OBSAH

SEZNAM POUŽITÝCH POJMŮ A ZKRATEK

Active	Je řešení adresářových služeb pro správu síťových prostředků.
Directory	Active Directory využívají administrátoři počítačových sítí pro různé účely. Nastavují za jeho pomoci pravidla a politiku sítě, instalují programy na veliké množství PC stanic zároveň či řeší kritické situace v síti.
Administrátor	Osoba pověřená správou jednoho, nebo více ICT zařízení, která je schválena ředitelem organizace a má nejvyšší úroveň oprávnění pro ICT zařízení ve své správě.
Administrátorský účet	Uživatelský učet, jenž má nevyšší možná oprávnění v rámci daného operačního systému nebo aplikace.
Aplikace	Programové vybavení výpočetní techniky organizace (např. MS Word).
Autentizace	Je proces ověření proklamované identity subjektu.
Bezpečnost informací	Je zajištění následujících atributů chráněných informací: důvěrnosti (ochrana před neoprávněným čtením), integrity (ochrana před neoprávněnými úpravami nebo zničením) a dostupnosti (zajištění adekvátního přístupu a ochrana před jeho neoprávněným zamezením).
Cloud	Externí internetové datové uložiště (např. One Drive, Google drive, Dropbox apod.).
Fyzická bezpečnost	Fyzická bezpečnost znamená používání fyzických a technických ochranných opatření k zamezení neoprávněného přístupu k majetku a informacím organizace.
Garant aplikace	Zaměstnanec odpovědný za konkrétní aplikaci. Garant aplikace je odborný zaměstnanec se znalostí dané aplikace a rozhoduje o požadavcích na přístup k dané aplikaci.
Hardware	Označuje veškeré fyzicky existující technické vybavení výpočetní techniky či síťových prostředků.
Operační systém	Základní programové vybavení počítače (tj. software), který je zaveden do paměti počítače při jeho startu a zůstává v činnosti až do jeho vypnutí (např. MS Windows 10).

PREAMBULE

Role definované tímto dokumentem předpokládají, že je bude vykonávat i žena. Avšak z důvodu zjednodušení textu jsou použity názvy jednotlivých rolí v mužském rodě. Bude-li danou roli zajišťovat žena, předpokládá se automatické přechylování názvů jednotlivých rolí. bez nutnosti úpravy směrnice.

1 PŮSOBNOST DOKUMENTU

Tento dokument stanovuje bezpečnostní pravidla pro zpracování, uchování a předávání dat organizace, obsahující osobní údaje v souladu s požadavky *Nařízení evropského parlamentu a rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES* (dále jen GDPR).

Dokument je platný pro všechny zaměstnance organizace. Bezpečnostní pravidla, definovaná tímto dokumentem, jsou platná pro zpracování dat, obsahujících osobní údaje ve všech operačních systémech a aplikacích, které jsou ve správě organizace a provozované buď na výpočetní technice příspěvkové organizace, nebo na technice a aplikacích poskytnutých smluvním dodavatelem.

2 ÚVOD

 Úroveň bezpečnosti 1 – minimální bezpečnostní požadavky platné pro všechny organizace bez rozdílu svého zaměření. Jsou zde zařazeny organizace, které používají pouze koncové počítače a nemají serverová řešení. Většinu svých agend zpracovávají v základních aplikacích pro Windows (např. MS Office) nebo v rámci on-line dodavatelských řešení, tzv. pomocí webového prohlížeče. Síťová infrastruktura existuje jen pro připojení do sítě Internet, případně sdílený tisk a obsahuje pouze několik jednotek pracovních stanic nebo notebooků.

3 ORGANIZACE BEZPEČNOSTI

Ředitel organizace je odpovědný za ustanovení zaměstnanců do jednotlivých rolí, ve kterých budou odpovědni za řízení bezpečnosti osobních údajů. Jedná se především o ustanovení role pověřence pro ochranu osobních údajů, správců ICT, administrátorů a jednotlivých garantů aplikací. Schvaluje také přidělení administrátorských účtů vybraným zaměstnancům.

4 BEZPEČNOSTNÍ PRAVIDLA UŽIVATELŮ

Zaměstnanci jsou povinni dodržovat následující bezpečnostní pravidla při zpracovávání osobních údajů:

1) Svěřenou výpočetní techniku využívají pouze pro plnění pracovních povinností.

2) Dodržují zásady pro tvorbu přístupového hesla k operačním systémům a/nebo aplikacím.

3) Zachovávají jedinečnost a důvěrnost přístupového hesla, tj. nikomu heslo nesdělují a nikde a nijak si jej nezaznamenávají.

4) Při přihlašování k operačním systémům nebo aplikacím dbají na to, aby nebylo možné heslo odpozorovat další osobou.

5) V případě jakéhokoliv podezření na kompromitaci hesla nebo dokonce jeho zneužití heslo okamžitě změní.

6) Před opuštěním pracoviště zabezpečují výpočetní techniku uzamčením pracovní plochy nebo odhlášením (např. pomocí kláves ⊞+L nebo ctrl+alt+del).

7) Dodržují pravidlo „prázdného stolu“, to znamená, že všechny dokumenty obsahující osobní údaje, které v danou chvíli nezpracovávají, jsou uloženy v uzamykatelných skříních.

8) Při používání přenosné výpočetní techniky a datových nosičů (notebooků, flash disků, externích HDD, DVD apod.) mimo prostory organizace:

a. nepředávají tuto techniku a nosiče třetím osobám,

b. učiní všechna dostupná opatření která mohou zabránit ztrátě či odcizení výpočetní techniky (neponechávají je bez dohledu a/nebo zabezpečení např. v dopravních prostředcích, v ubytovacích zařízeních apod.),

c. nepoužívají výpočetní techniku na veřejných místech pro práci s daty organizace,

d. ztrátu či odcizení okamžitě nahlásí svému nadřízenému.

9) Neinstalují software na výpočetní techniku organizace.

10) Nepoužívají soukromé datové nosiče (např. CD, flash disky, externí HDD).

11) Nenavštěvují rizikové internetové stránky.

12) Důsledně ověřují doručenou elektronickou poštu a v případě podezření, že se jedná o závadný e-mail (spam, podvodný e-mail apod.), takovou zprávu neotvírají, nereagují na ní a tuto skutečnost neprodleně ohlásí správci ICT.

13) Nezasahují do výpočetní techniky a její konfigurace, vyjma situací, kdy toto bude vyžadováno přímo správcem ICT.

14) Odpovídají za zálohování dat na přidělené výpočetní technice.

15) Nekopírují, neukládají, nepřenáší osobní údaje a data z aplikací organizace na pevných discích počítačů, jiných datových nosičích či cloudu, vyjma stanovených úkolů a povinností či po schválení ředitelem organizace.

16) Soubory, obsahující osobní údaje, adresované mimo doménu příspěvkové organizace zasílat pouze chráněné (prostřednictvím datových schránek, nebo prostřednictvím elektronické pošty minimálně v archivním souboru (např. ve formátu „zip“, „rar“ atd.) opatřeného heslem, přičemž heslo zaslat adresátovi jiným komunikačním kanálem, např. prostřednictvím SMS).

17) Soubory, obsahující zvláštní kategorie osobních údajů, zasílat pouze prostřednictvím datové schránky.

18) Netisknou data z aplikací organizace pro jiné než pracovní účely.

19) Pokud dojde k úniku, kompromitaci nebo ztrátě dat obsahujících osobní údaje je každý zaměstnanec povinen neprodleně hlásit tento incident nadřízenému vedoucímu zaměstnanci, který tuto skutečnost hlásí neprodleně pověřenci pro ochranu osobních údajů.

5 BEZPEČNOSTNÍ PRAVIDLA SPRÁVCE ICT

Správce ICT je odpovědný za dodržování bezpečnostních pravidel při zpracovávání a ochraně osobních údajů v rámci počítačové sítě a na výpočetní technice organizace. Je povinen dodržovat následující bezpečnostní pravidla při plnění pracovních úkolů správce ICT:

1) Spolupracuje s organizací na tvorbě a aktualizaci analýzy rizik.

2) Spravuje antivirový systém na všech výpočetních prostředcích organizace a to především:

a. provádí jeho instalaci,

b. kontroluje funkčnost aktualizací,

c. kontroluje výstupy programu.

3) Pro zaměstnance organizace připravuje a instaluje výpočetní techniku, kterou nastaví dle definovaných bezpečnostních požadavků (např. způsoby přihlášení, oprávnění uživatelského účtu, uzamykání počítače při neaktivitě apod.) a následně ji předává určeným zaměstnancům k použití.

4) Vytváří a nastavuje zaměstnancům uživatelská oprávnění do počítačové sítě a aplikací v rozsahu schváleném ředitelem.

5) Na základě požadavku ředitele organizace zřizuje nebo ruší přístupy do operačních systémů organizace.

6) Na základě požadavku garanta aplikace zřizuje nebo ruší přístupy do aplikace organizace.

7) Zajišťuje fyzickou bezpečnost datových úložišť, nosičů a dat organizace.

8) Poskytuje zaměstnancům organizace technickou podporu při využívaní výpočetní techniky.

9) Provádí kontrolní činnost k zajištění bezpečnosti osobních údajů zpracovávaných ve výpočetní technice organizace.

10) Vede provozní deník, ve kterém zaznamenává všechny klíčové činnosti související se správou počítačové sítě organizace.

11) Provádí bezpečnou likvidaci datových nosičů organizace, zejména pak pevných disků, flash disků, paměťových karet, CD a DVD disků apod.

12) V případě nutnosti odeslat výpočetní techniku či jejich komponenty obsahující osobní údaje mimo organizaci (oprava u servisní organizace, výpůjčka, pronájem, vyřazení,

likvidace apod.), musí před odesláním vymazat z pevného disku veškeré osobní údaje nebo musí vyjmout paměťová média.

13) Provádí zálohování zpracovávaných dat a klíčových síťových prostředků organizace tak, aby při selhání např. hlavního datového úložiště, bylo možné provést obnovu dat s minimální ztrátou uložených dat.

6 ŘÍZENÍ RIZIK

Organizace provádí v pravidelných intervalech analýzu rizik v souladu s metodikou pro analýzu rizik na základě požadavků čl. 24 a 32 GDPR.
Analýza rizik GDPR má za cíl určit možné hrozby a zranitelnosti při zpracování osobních údajů, včetně identifikace a stanovení rizik, která mohou vzniknout působením těchto hrozeb na účely zpracování osobních údajů.

7 ŘÍZENÍ AKTIV

Ředitelem pověřená osoba eviduje veškerý hardware a aplikace používané organizací.
Používání soukromých přenosných paměťových zařízení (externí pevné disky a flash disky) pro ukládání nebo zpracování osobních údajů je zakázáno.
Veškerá výpočetní technika organizace disponuje aktuálním operačním systémem a aplikacemi, jež mají nastavené automatické aktualizace.
Při přidělení výpočetní techniky jinému zaměstnanci správce ICT provádí kompletní reinstalaci, pokud je to nutné. Ředitel nebo jím pověřená osoba určí, jakým způsobem naložit s daty, která jsou na výpočetní technice uložena.

8 ŘÍZENÍ PŘÍSTUPŮ

Každý zaměstnanec využívající výpočetní techniku organizace, používá pro připojení k operačním systémům a aplikacím jedinečné uživatelské jméno a heslo.
Společné, projektové či jinak sdílené uživatelské účty k operačním systémům a aplikacím obsahující osobní údaje jsou zakázány.
Všem zaměstnancům organizace jsou standardně přidělovány základní uživatelské účty.
Přístup ke sdíleným složkám je zaměstnancům povolen pouze na základě zadání jejich uživatelského jména a hesla. Správce ICT definuje způsoby přístupu k těmto složkám a na základě schválení ředitele nastaví příslušná přístupová oprávnění jednotlivým uživatelům.
Administrátorské účty jsou striktně řízeny. Správce ICT na základě souhlasu ředitele organizace nastavuje přístupy tak, aby administrátorským účtem disponovali jen zaměstnanci, kteří jej ke své práci prokazatelně potřebují (správci ICT apod.).
Zaměstnanci s administrátorskými účty jsou prokazatelně seznámeni s faktem, že jsou majiteli administrátorského účtu a jsou si vědomi vyšších bezpečnostních a uživatelských nároků spojených s tímto typem účtu.
Zaměstnanci s administrátorskými účty jsou pro běžnou práci povinni používat standardní uživatelský účet. Administrátorský účet jsou oprávněni použít pouze v opodstatněných případech k výkonu činností, pro které je toto oprávnění nezbytné.
Správce ICT vede seznamy zaměstnanců, kteří disponují administrátorskými účty. Ředitel organizace, ve spolupráci se správcem ICT, pravidelně tyto seznamy přezkoumává z hlediska aktuálnosti a potřebnosti
Garanti aplikací jsou odpovědní za řízení přístupových oprávnění zaměstnanců ke svěřeným aplikacím.
Garanti aplikací spolupracují se správcem ICT na pravidelném přezkoumávání přístupových oprávnění do aplikací.
Při nástupu zaměstnance jsou správcem ICT, na základě pokynů ředitele organizace a garanta aplikace, nastupujícímu zaměstnanci přiděleny uživatelské účty a přístupové údaje k operačním systémům a aplikacím organizace.
Při vzniku potřeby změnit přidělená přístupová opatření, žádá zaměstnanec nebo jeho přímí nadřízený příslušného garanta aplikace o povolení požadovaných přístupových oprávnění.
V případě ukončení pracovního poměru zaměstnance jsou na základě pokynu ředitele veškerá přístupová oprávnění zaměstnance odebrána správcem ICT.
Na veškeré výpočetní technice organizace je nastaveno uzamykání uživatelského účtu max. po 45 min. jeho neaktivity.

Mobilní zařízení organizace jsou chráněna proti neoprávněnému přístupu heslem, gestem, pinem nebo otiskem prstu.
Minimální pravidla pro hesla uživatelů jsou stanovena následovně:
a) minimální délka je 8 znaků, obsahující alespoň jednu číslici a velké písmeno,

b) minimální doba platnosti hesla je 1 hodina,

c) maximální platnost hesla je nastavena na 6 měsíců s vynucenou změnou (tj. nelze ji odložit),

d) nelze použít 3 poslední zadaná hesla.

Pokud je to technicky možné, operační systémy a aplikace organizace jsou nastaveny tak, aby neumožňovaly uživatelům měnit minimální požadavky na kvalitu hesla.
Administrátorské účty a správce ICT pro přihlašování k síťovým prostředkům používá heslo splňující alespoň následující pravidla:
a) minimální délka 15 znaků, obsahuje alespoň jednu číslici, malé a velké písmeno,

b) minimální doba platnosti hesla je 1 den,

c) maximální platnost hesla je nastavena na 6 měsíců s vynucenou změnou (tj. nelze ji odložit),

d) nelze použít 3 posledních použitých hesel.

9 FYZICKÁ BEZPEČNOST

Organizace má definovaná režimová opatření pro provoz budov organizace.
Zaměstnanci, zacházející s písemnostmi, obsahujícími osobní údaje, mají dostatek uzamykatelných úložných prostor pro ukládání těchto dokumentů, která aktivně využívají.
V organizaci je stanoven klíčový režim (tzn. klíče, přidělené zaměstnancům, jsou evidovány).
Duplikáty klíčů jsou uloženy v trezoru nebo uzamykatelné skříňce.
Úklid prostor organizace je prováděn vlastními zaměstnanci. Pokud jsou pro úklid využívány služby externího dodavatele, je úklid prostor, obsahující písemnosti s osobními údaji, prováděn za přítomnosti zaměstnanců organizace.

10 NAKLÁDÁNÍ S OSOBNÍMI ÚDAJI

Data, obsahující osobní údaje, ukládají zaměstnanci do určených adresářů na interní pevný disk přidělené výpočetní techniky. Ukládat osobní údaje na soukromá paměťová média a do nezabezpečeného cloudu je zakázáno.
Soubory, obsahující osobní údaje, jsou primárně zasílány mimo organizaci prostřednictvím datové schránky. Pokud tak nelze učinit, musí zaměstnanec tento soubor uložit do souboru typu ZIP, RAR apod. zabezpečeného heslem, který je odeslán příjemci elektronickou poštou. Heslo je příjemci zasláno jiným komunikačním kanálem např. SMS. Pro zašifrování souboru je možné využít kvalifikovaný certifikát.
Soubory, obsahující zvláštní kategorie osobních údajů, jsou zasílány pouze prostřednictvím datové schránky.
Zaměstnanci, zpracovávající dokumenty obsahující osobní údaje, musí mít možnost zabezpečeného tisku. První možností je tisk na osobních tiskárnách umístěných v kanceláři zaměstnance. Druhou možností je tisk dokumentů na společných tiskárnách, umístěných mimo místnost zaměstnance, pomocí zadání osobního kódu zaměstnance nebo přiložením identifikačního čipu k tiskárně.
Pro ukládání osobních údajů na přenosná paměťová zařízení (flash a externí pevné disky) nebo notebooky je vždy využito šifrování. Např. za pomoci softwaru BitLocker integrovaného do operačního systému Windows 10 ve verzi Professional a vyšší nebo jiného vhodného šifrovacího nástroje či kvalifikovaného certifikátu.
Paměťová zařízení, obsahující zálohy dat organizace, jsou uchovávána v uzamykatelných skříních a nejsou používána pro jiný účel.

11 BEZPEČNOST SÍTĚ

Wi-Fi síť organizace je používána jen pro přístup do sítě Internet. Je chráněna standardními prostředky včetně přístupového hesla. Heslo pro přístup do sítě Wi-Fi je pravidelně měněno 1x za 6 měsíců. Minimální požadavky na kvalitu hesla jsou definovány v kapitole Řízení přístupů (Úroveň 1).
V nastavení přístupových údajů k administraci routerů musí odpovědná osoba změnit továrně nastavené přístupové údaje. Kvalita nového hesla splňuje požadavky pro heslo správce ICT (Úroveň 2).
Mobilní zařízení organizace (smartphony, tablety) s vlastním operačním systémem jsou vybavena antivirovou aplikací.
Zaměstnanci mohou využívat soukromá mobilní zařízení pouze pro práci s obsahem pracovní emailové schránky. Jiné využití soukromých mobilních zařízení pro pracovní účely (např. připojení do vnitřní sítě organizace, administrace aplikací apod.) je zakázáno.

12 DODAVATELÉ SLUŽEB ICT

Organizace identifikuje dodavatele aplikací a služeb ICT s možností přístupu k datům organizace (i vzdálený přístup např. pomocí VPN) a uzavře s nimi smlouvy, příp. dodatek smlouvy o zpracování osobních údajů v souladu s požadavky čl. 28 GDPR.
Správce ICT eviduje jednotlivé vzdálené přístupy dodavatelů a kontroluje jejich oprávněnost.

.....
Mgr. Bohumil Herčík
ředitel školy