Mateřská škola, základní škola a praktická škola Znojmo, příspěvková organizace	
OCHRANA DAT ZPRACOVANÝCH VÝPOČETNÍ TECHNIKOU	
Č.j.: MZPSZN- 886/2019	**I/1.3 A 5**
Vypracoval:	Mgr. Jiří Šrůtka, metodik a koordinátor ICT
Schválil:	Mgr. Ludmila Falcová, ředitelka školy
Směrnice nabývá platnosti ode dne:	4.10.2019
Směrnice nabývá účinnosti ode dne:	4.10.2019

Obecná ustanovení

Na základě ustanovení § 248 zákona č. 262/2006 Sb., zákoníku práce a zákona č. 110/2019 Sb., o zpracování osobních údajů a podle nařízení Evropského parlamentu a Rady (EU) 2016/679 vydávám jako statutární orgán organizace tuto směrnici.

1 Působnost a zásady směrnice

Směrnice upravuje povinnosti zaměstnanců organizace při ochraně údajů zpracovávaných organizací. Zásady směrnice

a) tento předpis ukládá povinnosti všem zaměstnancům organizace,
b) je vydáván písemně,
c) nesmí být vydán v rozporu s právními předpisy,
d) nesmí být vydán se zpětnou účinností,
e) vzniká na dobu neurčitou,
f) ředitel školy seznamuje zaměstnance s vydáním, změnou nebo zrušením této směrnice
g) prokazatelným způsobem, v organizaci obvyklým,
h) směrnice je přístupná všem zaměstnancům zveřejněním na místě obvyklém.

2 Pořizování, ukládání a zpracování dat.

a) Zpracováním dat se rozumí jakákoliv operace nebo soustava operací, které jsou systematicky prováděny s osobními údaji, bez ohledu na to, zda automatizovaně nebo jinými prostředky. Zejména se jedná o shromažďování, ukládání na nosiče informací, zpřístupňování, úpravu nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměnu, třídění nebo kombinování, blokování a likvidaci takových údajů.
b) Za obsahovou správnost, kompletnost a následné uloženi dat v počítačové evidenci v okamžiku pořízení (změny) zodpovídá vždy ten, kdo data pořídil (změnil), bez ohledu na to, odkud byla data získána, a v či pracovní náplni je sběr a zpracovaní těchto dat. Zaměstnanec, zadávající údaje do počítačové evidence, je povinen vždy si řádně ověřit věrohodnost a správnost těchto údajů. Zaměstnanec, který zjistí nesrovnalost mezi aktuálně zjištěným údajem a údajem v počítačové evidenci, je povinen tuto skutečnost neprodleně ohlásit příslušnému správci daného údaje a spolupodílet se na zajištění nápravy.

3 Ochrana dat

a) Smyslem ochrany dat je učinit taková organizační a technická opatření, která v nejvyšší možné míře omezí možnost nenávratného poškození nebo ztráty dat, minimalizují negativní dopady, způsobené poškozením nebo ztrátou dat, na další činnost organizace. Přijata opatřeni zamezí přístup k datům nepovolanými osobami.
b) Předmětem ochrany jsou veškeré programové vybavení včetně doprovodné dokumentace, všechna provozní data uložená na nosičích informaci, v operační paměti počítačů, tiskáren a dalších zařízení výpočetní techniky, záložní a archivní kopie dat uložené na nosičích informaci, údaje zobrazené nebo vytištěné na výstupních zařízeních; přístupová hesla, technické informace o informačním systému a návody.
c) Všichni zaměstnanci, přicházející do styku s výpočetní technikou, jsou povinni učinit a průběžně dodržovat taková bezpečnostní opatření, která v maximální možné míře vyloučí nenávratnou ztrátu a trvalé poškození provozních dat, která by mohla být způsobena náhodným nebo úmyslným zásahem další osoby, neodbornou obsluhou, poruchou VT, požárem, živelní pohromou, atp.
d) Provozní data, uložena na pevných discích počítačů musí být zálohována v počítačové síti, popřípadě na dalších nosičích informaci. V případě zálohování dat uložených na lokálním disku osobního počítače musí být data zálohována v minimálně dvou od sebe oddělených kopiích.
e) Vytvořeni záložní kopie je nutno zajistit (aktualizovat) při jakémkoli pořízení (změně) provozních dat v počítačové evidenci. Pokud nejsou provozní data v průběhu pořízení (aktualizace) ukládána na disk serveru (centrálního počítače), ale pouze lokálně na disk osobního počítače, odpovídá za pořízení záložní kopie provozních dat vždy ten, kdo data pořídil (změnil), bez ohledu na to, odkud byla data získána a v či pracovní náplni je sběr a zpracování těchto dat. Záložní kopie dat je v těchto případech nutno pořídit (aktualizovat) nejpozději před ukončením pracovní směny v den, kdy byla provozní data pořízena (změněna). Pokud jsou provozní data v průběhu pořízení (aktualizace) ukládána na disk serveru (centrálního počítače), odpovídá za pořízení záložní kopie provozních dat správce. Záložní kopie provozních dat je pořizována automatizovaně.
f) Mezi způsoby ochrany patří zejména - znemožnění jakéhokoli přístupu nepovolaných osob k výpočetní technice a datům, a to jak v pracovní, tak i v mimopracovní době. Neponechávání zapnuté techniky bez dozoru. Situování pracoviště tak, aby nebylo možno odečítat údaje z monitorů nepovolanými osobami. Uloženi tiskových výstupů mimo dosah nepovolaných osob. Ochrana přístupovým heslem, udržováni hesla v tajnosti, častá změna hesla. Heslo je tvořeno nejméně osmi znaky, vždy obsahuje kombinaci číslic, malých a velkých písmen, nejde o snadno odhalitelný text obsahující jména, příjmení, data narození. Důsledné odhlašováni se z počítačové sítě při delší nepřítomnosti na pracovišti. Není dovoleno přesunovat, odpojovat, přenášet, připojovat a ani jinak manipulovat s umístěným zařízením.
g) Na počítačích mohou pracovat pouze zaměstnanci k tomu pověření. Počítače, na kterých je zpracováváno účetnictví, mzdová agenda a personalistika, chrání příslušní zaměstnanci před neoprávněným přístupem, zpravidla přístupovými hesla, uzamčením. Mimo běžnou pracovní dobu je místnost zabezpečena elektronickým zabezpečovacím systémem.
h) Jakoukoli závadu nebo i podezření na nestandardní fungování počítače zaměstnanec bez zbytečného odkladu hlásí svému nadřízenému nebo pověřenému zaměstnanci. Do odstranění závady nebo prověření nezávadného stavu nesmí zaměstnanci používat technické zařízení v síti (např. v systému elektronického bankovnictví).
i) Správce sítě je oprávněn v rámci své kompetence monitorovat vytížení sítě a oprávněnost využívání jednotlivými uživateli. Toto ustanovení může být využíváno pro identifikaci přestupků uživatelů v souladu s platnou právní úpravou.

4. Zásady pro práci na výpočetní technice

a) Je zakázáno používat nelegální software; používat software, jehož použití nebylo schváleno správcem ICT, instalovat bez svolení správce ICT na disky počítačů jakýkoliv software či data s tímto programovým vybavením související, odstraňovat instalovaný software, provádět změny v nastavení a umístění software a souvisejících dat, pořizovat kopie software a dat pro jinou, než služební potřebu, předávat data jiným subjektům bez předchozího souhlasu příslušného vedoucího pracovníka, provádět demontáž, úpravy, opravy, změny v nastaveni a zapojeni prostředků ICT, používat prostředky ICT pro jiné, než schválené účely, instalovat a hrát počítačové hry.

b) Při zahájení práce s ICT je zaměstnanec povinen překontrolovat stav a kompletnost svěřených prostředků výpočetní techniky. Ukončování činnosti programů se provádí předepsaným způsobem, včetně ukončení práce v síti. Před odchodem zaměstnance z pracoviště musí být všechny jemu svěřené prostředky, tj. osobni počítače, tiskárny, modemy, atd., vypnuty, s výjimkou těch zařízení, která musí zůstat s ohledem na své určeni trvale zapnuta.

c) Při ukončení nebo změně pracovně právního vztahu správce sítě provede úpravu uživatelského účtu pracovníka, včetně přístupových práv.

d) Tiskové výstupy obsahující data podléhající ochraně osobních údajů musí příslušný pracovník zabezpečit před neoprávněným přístupem.

5. Archivace, skartace dat

a) Pro archivaci dat se v organizaci používají místní síťové (serverové) uložiště. Technické nosiče jsou uschovávány pouze na pracovištích organizace, v uzamykatelných skříních. Jsou ukládány vždy v jiné místnosti, než originální údaje. Není-li uvedeno jinak, ukládají se zálohy vybraných aplikací na dvou místech: na serverech WWWLNX a WIN2K. Pro přenos dat se v organizaci používá intranetová síť. USB flash disky, CD-ROM (DVD) pro archivaci nejsou dovoleny.

b) Každý zaměstnanec je povinen provádět zálohování dat podle rozpisu zálohování. Denně jsou zálohována data v účetnictví. Týdně jsou zálohována data, ze kterých jsou vytvářeny tiskové výstupy. Zaměstnanci uchovávají osobní data na intranetu v určené složce chráněné heslem, aby je bylo možné snadno zálohovat.

c) Zálohována jsou všechna data, nikoli programy nebo operační systém. Zálohy jsou ukládány mimo místnost, kde je počítač umístěn (aby zálohy nemohly být odcizeny nebo poškozeny spolu s počítačem, který je zálohován).

d) Je prováděna vždy plná záloha, kompletní kopie všech zálohovaných dat, nikoli jen tzv. přírůstková záloha (data, která se změnila od poslední plné zálohy).

e) Zálohování dat se provádí vždy při ukončení pracovně právního vztahu pracovníka.

f) Na základě ustanovení § 32 zákona č. 563/1991 Sb. o účetnictví, v platném znění se doklady osvědčující legální nabytí software uchovávají po celou dobu užívání licence, není možné je skartovat spolu s ostatními doklady v účetnictví. Z tohoto důvodu správce ICT vede v součinnosti s účetní organizace evidenci všech typů licencí s odkazy na účetní doklady a evidenci umístění instalačních médií a souvisejících tiskovin – manuálů.

Doklad o nabytí software musí obsahovat jasnou identifikaci dodavatele a odběratele, datum nabytí, specifikaci produktu včetně čísla verze a jazykové mutace, počet licencí.

g) Správce ICT vede přehled o instalaci software na jednotlivé pracovní stanice a jeho kontrolách. Jakékoli porušení této směrnice hlásí svému vedoucímu pracovníkovi.

6. Na všech počítačích organizace je používán jeden typ antivirového programu, je nastaven tak, aby jeho aktualizace byly prováděny automaticky prostřednictvím internetu.

7. Na počítačích organizace je dovoleno používat pouze legálně pořízený software. Instalaci a aktualizace programů provádí pouze pověřený zaměstnanec. Pro ostatní zaměstnance platí zákaz manipulace s instalovanými programy, změny konfigurace, nelegální pořizování kopií programů.

8. Kromě statistických sledování a hlášení nadřízeným orgánům je zakázáno poskytovat přes internet údaje o škole a zaměstnancích.

9. Externí pracovníci, nebo dodavatelé služeb, zejména účetní a mzdová účetní, odevzdávají výstupy své práce vždy i v elektronické podobě.

10. Zaměstnanci mají přiděleny služební e-mailové adresy ve formátu

příjmení tečka spsznojmo@iskola.cz

Je zakázáno nastavovat automatické přeposílání došlých i odesílaných e-mailů na soukromé e-mailové adresy zaměstnanců.

11. Zaměstnanci jsou při zpracování dat povinni zachovávat mlčenlivost a chránit před zneužitím data, údaje a osobní údaje, se kterými byli seznámeni, vyžadovat a shromažďovat pouze nezbytné údaje a osobní údaje, bezpečně je ukládat a chránit před neoprávněným přístupem, neposkytovat je subjektům, které na ně nemají zákonný nárok, nepotřebné údaje vyřazovat a dál nezpracovávat.

12. Počítačová (kybernetická) bezpečnost

Je zajišťována na všech počítačích organizace
- instalací antivirových programů, firewallu,
- stanovením přístupových práv, hesel, zákazu sdílení hesel několika osobami,
- pravidelné zálohování dat, tak aby nedošlo k jejich ztrátě při případném odcizení či poruše počítače a byla zajištěna schopnost obnovy dat v případě fyzických či technických incidentů,
- zajištění automatických bezpečnostních aktualizací používaného software,
- při jakékoli likvidaci hardware musí být znemožněna možnost získání uložených osobních údajů,
- používání pouze silných hesel (heslo o délce minimálně osmi znaků, vždy musí jít o kombinaci malých a velkých písmen a čísel, případně zvláštních znaků)
- mazání a neotvírání nevyžádané pošty, odmazávání SPAM v emailové schránce i v počítačích,
- pravidelný servis a výpočetní techniky je zaměřen i na kontrolu oblasti bezpečnosti dat,
je prováděno pravidelné testování přijatých technických a organizačních opatření,
- pravidelným školením zaměstnanců v této oblasti,
- vhodnou pracovní náplní metodika ICT (n.v.č. 75/2005 Sb., a koordinátora ICT (v.č. 317/2005).
- v nastavení správy e-mailových účtů je zakázána možnost přeposlání obsahu pracovních e-mailů na soukromé.

13. Závěrečná ustanovení

a) Kontrolou provádění ustanovení této směrnice je statutárním orgánem školy pověřen metodik a koordinátor ICT – Mgr. Jiří Šrůtka.
b) Zrušuje se předchozí znění této směrnice – MZPSZN-631/2016. Uložení směrnice se řídí spisovým řádem školy.
c) Směrnice nabývá platnosti dne 4.10.2019
d) Směrnice nabývá účinnosti dne 4.10.2019

Znojmo, 4.10.2019

Mgr. Ludmila Falcová
ředitelka školy