ZÁKLADNÍ ŠKOLA BŘECLAV, SLOVÁCKÁ 40

příspěvková organizace

SMĚRNICE O BEZPEČNOSTI ICT

Číslo jednací:	ZSSL- 51/2019
Vypracovala:	Mgr. Iva Jobánková, ředitelka školy
Platnost od:	1.3.2019

Směrnice o bezpečnosti ICT

Článek I
Organizace bezpečnosti

1.1 Za ustanovení jednotlivých rolí zaměstnanců, v nich budou odpovědní za zajištění bezpečnosti a ochrany osobních údajů, odpovídá ředitel Základní škola Břeclav, Slovácká 40, p.o.
Jedná se především o ustanovení role:

- pověřence pro ochranu osobních údajů – Město Břeclav
- správce ICT,
- administrátorů a
- jednotlivých garantů aplikací.

1.2 Ředitel školy schvaluje také přidělení administrátorských účtů vybraným zaměstnancům.

Článek II
Bezpečnostní pravidla uživatelů

2.1 Zaměstnanci jsou povinni dodržovat při zpracovávání osobních údajů tato pravidla:

1. Výpočetní techniku využívají pouze pro plnění pracovních povinností.
2. Dodržují zásady pro tvorbu přístupového hesla k operačním systémům a aplikacím.
    a. zachovávají jedinečnost, bezpečnost a důvěrnost přístupového hesla, nikomu heslo nesdělují a nikde a nijak si jej nezaznamenávají.
    b. při přihlašování k operačním systémům a aplikacím dbají na to, aby nebylo možné heslo odpozorovat další osobou.
    c. v případě jakéhokoliv podezření na kompromitaci hesla nebo dokonce jeho zneužití heslo okamžitě změní, požádají příslušnou osobu o provedení změny a informují vedení školy. O změně hesla bude proveden písemný záznam.
3. Před opuštěním pracoviště zabezpečují výpočetní techniku uzamčením pracovní plochy nebo odhlášením.
4. Dodržují pravidlo „prázdného stolu“ - všechny dokumenty obsahující osobní údaje, které v danou chvíli nezpracovávají, jsou uloženy v uzamykatelných skříních.
5. 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,
    c. nepoužívají výpočetní techniku pro práci s daty organizace na veřejných místech,
    d. ztrátu či odcizení okamžitě nahlásí svému nadřízenému.
6. Na výpočetní techniku školy neinstalují žádný software.
7. Nepoužívají soukromé datové nosiče (např. CD, flash disky, externí HDD).
8. Nenavštěvují rizikové internetové stránky.
9. 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.
10. Nezasahují do výpočetní techniky a její konfigurace.
11. Nekopírují, neukládají, nepřenáší osobní údaje a data z aplikací organizace na pevných discích počítačů, jiných datových nosičích či cloudu.

12. Soubory, obsahující osobní údaje, adresované mimo doménu *Břeclav, Slovácká 40,p.o.*, budou zasílány výhradně vedením školy pouze chráněné
    a. prostřednictvím datových schránek,
    b. prostřednictvím elektronické pošty v archivním souboru (např. ve formátu „zip“, „rar“ atd.) opatřeného heslem - heslo zaslat adresátovi jiným komunikačním kanálem, např. prostřednictvím SMS).
13. Soubory, obsahující zvláštní kategorie osobních údajů, zasílat pouze prostřednictvím datové schránky.
14. Netisknou data z aplikací organizace pro jiné než pracovní účely.
15. Pokud dojde k úniku, kompromitaci nebo ztrátě dat obsahujících osobní údaje je každý zaměstnanec povinen neprodleně hlásit tento incident písemně neprodleně pověřenci pro ochranu osobních údajů.

Článek III
Bezpečnost pravidla správce ICT

3.1 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. 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.
    a. způsoby přihlášení,
    b. oprávnění uživatelského účtu,
    c. 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 využívání výpočetní techniky.
9. Provádí kontrolní činnost k zajištění bezpečnosti osobních údajů zpracovávaných ve výpočetní technice organizace.
10. Vede dokumentaci, serverové a síťové infrastruktury, ve které 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 předání výpočetní techniky nebo jejich komponentů obsahujících osobní údaje mimo organizaci (oprava u servisní organizace, výpůjčka, pronájem, vyřazení, likvidace apod.), vyjme paměťová média nebo vymaže veškeré osobní údaje.

13. Provádí pravidelné 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.

Článek IV
Řízení rizik

4.1 Organizace provádí v pravidelných intervalech (alespoň jedenkrát za rok) analýzu rizik 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.

Článek V
Řízení aktiv

5.1 Škola eviduje veškerý hardware a software, který používá.
5.2 Používání soukromých přenosných paměťových zařízení (externí pevné disky a flash disky) pro ukládání nebo zpracování osobních údajů je zakázáno.
5.3 Paměťová zařízení, která ke své práci potřebují zaměstnanci, jsou evidována. Evidenci paměťových zařízení provádí správce ICT .
5.4 Veškerá výpočetní technika *Základní škola Břeclav, Slovácká 40, p.o.*disponuje aktuálním operačním systémem a aplikacemi, jež mají nastavené automatické aktualizace.
5.5 Při přidělení výpočetní techniky jinému zaměstnanci správce ICT provádí reinstalaci, případně vymazání citlivých dat, osobních údajů a uživatelských účtů ze zařízení. Ředitel nebo jím pověřená osoba určí, jakým způsobem naložit s daty, která jsou na výpočetní technice uložena.

Článek VI
Řízení přístupů

6.1 Každý zaměstnanec využívající výpočetní techniku školy, používá pro připojení k operačním systémům a aplikacím jedinečné uživatelské jméno a heslo.
6.2 Společné, projektové či jinak sdílené uživatelské účty k operačním systémům a aplikacím obsahující osobní údaje jsou zakázány.
6.3 Všem zaměstnancům organizace jsou standardně přidělovány standardní uživatelské účty.
6.4 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.
6.5 Administrátorské účty jsou striktně řízeny. Správce ICT na základě souhlasu ředitele organizace disponuje těmito administrátorskými účty a je oprávněn je použít pouze v opodstatněných případech k výkonu činností, pro které je toto oprávnění nezbytné.
6.6 Při nástupu zaměstnance jsou správcem ICT, na základě pokynů ředitele organizace nastupujícímu zaměstnanci přiděleny uživatelské účty a přístupové údaje k operačním systémům a aplikacím organizace.
6.7 Při vzniku potřeby změnit přidělená přístupová opatření, žádá zaměstnanec vedení nebo správce ICT o povolení a provedení změny požadovaných přístupových oprávnění.
6.8 V případě ukončení pracovního poměru zaměstnance jsou na základě pokynu ředitele veškerá přístupová oprávnění zaměstnance odebrána správcem ICT.
6.9 Na veškeré výpočetní technice organizace je nastaveno uzamykání uživatelského účtu max. po 30 min. jeho neaktivity.

6.10 Mobilní zařízení organizace jsou chráněna proti neoprávněnému přístupu heslem, gestem, pinem nebo otiskem prstu.
6.11 Minimální pravidla pro hesla uživatelů jsou stanovena následovně:

a. minimální délka je 7 znaků, obsahující alespoň jednu číslici a velké písmeno,
b. maximální platnost hesla je nastavena na 12 měsíců s vynucenou změnou (tj. nelze ji odložit),
c. 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.
6.12 Administrátorské účty a správce ICT pro přihlašování k síťovým prostředkům používá heslo splňující alespoň následující pravidla:

a. minimální délka 7 znaků, obsahuje alespoň jednu číslici, malé a velké písmeno,
b. maximální platnost hesla je nastavena na 12 měsíců s vynucenou změnou (tj. nelze ji odložit),
c. nelze použít 5 posledních použitých hesel.

Článek VII
Fyzická bezpečnost

7.1 Organizace má definovaná režimová opatření pro provoz budov organizace.
7.2 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 či místnosti.
7.3 Úklid prostor organizace je prováděn vlastními zaměstnanci.
7.4 Servery a jiná klíčová síťová zařízení jsou umístěny takovým způsobem, který maximálně zabraňuje nepovolaným osobám s těmito zařízeními jakkoliv manipulovat nebo je poškodit. Technologie jsou umístěny do uzamykatelných rackových skříní. Tyto skříně jsou, pokud možno, situovány v místnostech s omezeným vstupem osob.

Článek VIII
Nakládání s osobními údaji

8.1 Data, obsahující osobní údaje, ukládají zaměstnanci do určené síťové složky na serveru školy. Ukládat osobní údaje na soukromá paměťová média a do cloudu je zakázáno.
8.2 Soubory obsahující osobní údaje zasílá mimo organizaci výhradně vedení školy, a to buď prostřednictvím datové schránky, nebo musí 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.
8.3 Soubory, obsahující zvláštní kategorie osobních údajů, jsou zasílány pouze prostřednictvím datové schránky.
8.4 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.
8.5 Pedagogická dokumentace obsahující osobní údaje se bude tisknout pouze v kanceláři školy.

8.6 Pro ukládání osobních údajů na přenosná paměťová zařízení (flash a externí pevné disky) nebo notebooky je vždy využito šifrování za pomoci softwaru BitLocker integrovaného do operačního systému Windows 10 ve verzi Professional a vyšší nebo jiného vhodného šifrovacího nástroje či kvalifikovaného certifikátu.
8.7 Paměťová zařízení, obsahující zálohy dat organizace, jsou uchovávána v uzamykatelných skříních nebo místnostech a nejsou používána pro jiný účel.
8.8 Organizace má nastavený automatizovaný systém zálohování důležitých částí počítačové sítě včetně síťových prostředků.
8.9 Pokud jsou zálohy přenášeny mimo prostory organizace, je pro jejich ochranu využíváno šifrování.

Článek IX
Bezpečnost sítě

9.1 Wi-Fi síť organizace je používána pro přístup do sítě Internet. Je chráněna standardními prostředky včetně přístupového hesla. Minimální požadavky na kvalitu hesla jsou definovány v kapitole Řízení přístupů. Správce ICT nebo pověřený administrátor určuje, která zařízení se smí do sítě Wi-Fi připojit na základě filtrování MAC adres zařízení.
9.2 V nastavení přístupových údajů k administraci routerů musí odpovědná osoba změnit továrně nastavené přístupové údaje. Kvalita nového hesla splňuje požadavky pro heslo správce ICT.
9.3 Mobilní zařízení organizace (smartphony, tablety) s vlastním operačním systémem jsou vybavena antivirovou aplikací.
9.4 Zaměstnanci mohou používat svá mobilní zařízení v režimu BYOD, kdy budou zařízení připojena na Wi-Fi síť, která postkyje pouze konektivitu do internetu. Zaměstnanci mohou tuto konektivitu využívat pouze v průběhu a pro podporu výuky.
9.5 Wi-Fi síť je používána pro přístup k interní síti, a tedy i aplikacím organizace. Identita zaměstnance je před zpřístupněním této sítě ověřena prostřednictvím zadání přístupových údajů. Bez ověření identity zaměstnance nejsou interní síť, aplikace nebo síťové disky zpřístupněny.
9.6 Přístup k zálohám síťových prostředků a síťovým aplikacím je striktně omezen jak na logické, tak i fyzické úrovni pouze na odpovědné osoby.
9.7 Všechny vzdálené přístupy k síti organizace (pomocí např. vzdálené plochy nebo VPN) povoluje ředitel nebo správce ICT.
Všechny způsoby vzdáleného přístupu k síti organizace splňují následující:

a. vytvořené spojení v rámci vzdáleného přístupu je šifrované (bez ohledu na povahu přenášených dat) a předchází mu autentizace (minimálně heslem, lépe uživatelským certifikátem),
b. každý vzdálený přístup je jednoznačně identifikovatelný (uživatel) a je zaznamenán,
c. uživatelé nesmí „propůjčovat“ své oprávnění vzdáleného přístupu třetím osobám, byť zaměstnancům organizace,
d. připojení probíhá prostřednictvím bezpečného kanálu (HTTPS, VPN, pomocí VPN mimo veřejnou síť poskytovatele apod.).
e. Správce ICT vede evidenci zaměstnanců a výpočetní techniky s povoleným vzdáleným přístupem.

9.8 Pověřený administrátor přezkoumává v pravidelných intervalech (alespoň 1x za měsíc) důležité bezpečnostní logy firewallu. Například využití sítě (jednotlivých portů), neúspěšné pokusy o vzdálené přihlášení, pokusy o skenování sítě apod.

Článek X
Dodavatelé služeb ICT

10.1 Organizace uzavře s dodavateli aplikací a služeb ICT s možností přístupu k datům organizace smlouvy o zpracování osobních údajů.

10.2 Správce ICT eviduje jednotlivé vzdálené přístupy dodavatelů a kontroluje jejich oprávněnost.

10.3 V rámci smluvního vztahu s dodavatelem si organizace stanoví předmět dodávané služby. V rámci klasifikace úrovně dodávky musí být minimálně stanoveny následující podmínky:

a. stanovení předmětu a kvality služby,
b. stanovení Service Level Agreement SLA (pokud je předmětem dodávky služba),
c. stanovení požadavků na bezpečnostní opatření pro dodavatele a zároveň dodavatelského řetězce (pokud rizika závisí nejen na dodavateli, ale i na jeho subdodavatelích),
d. definice stížností, reklamací (stanovení postupů),
e. eskalační procedura (v případě, že nelze s dodavatelem dohodnout řešení, mělo by být určeno, na kterou hierarchicky vyšší řídící úroveň se řešení problému přesune),
f. nastavení kontrolních mechanizmů v rámci předmětu dodávané služby,
g. hodnocení a kontrola bezpečnostních opatření.

10.4 Za řízení dodavatelů je odpovědný ředitel školy nebo jím pověřená osoba, která danou službu za školu zastřešuje.

10.5 O všech změnách, dohodách a kontrolách s dodavateli bude proveden záznam.