Střední průmyslová škola elektrotechniky a informatiky, Ostrava, příspěvková organizace

Dokument:		PRAVIDLA PRO POUŽITÍ ŠKOLNÍ POČÍTAČOVÉ SÍTĚ SPŠEI	Počet stran: 2 Počet příloh: 0
Zpracoval:	Ing. Jan Patschka	Účinnost od: **1. 9. 2021**	Schváleno dne: 31. 8. 2021
Schválil:	Ing. Zbyněk Pospěch	Účinnost do: **trvalá**	Podpis:
Revize (datum změny):		Revizi provedl:	Podpis:

Pravidla pro použití školní počítačové sítě SPŠei

I.

Cílem pravidel pro použití školní počítačové sítě Střední průmyslové školy elektrotechniky a informatiky Ostrava (dále jen „SPŠei“) je vymezení činností a úkonů, které mohou jednotliví uživatelé realizovat.

II.

1) Pod pojmem *"počítačová síť"* (dále jen "síť") se rozumí všechny technické i programové prostředky používané k propojení a provozu počítačů. *"Uživatelem počítačové sítě"* (dále jen "uživatel") se rozumí každý, kdo přímo užívá výše zmíněné sítě. Za součást sítě je považováno technické vybavení počítače a jejich příslušenství, síťové prvky, tiskárny, programové vybavení a data.

2) Síť SPŠei je povoleno využívat výhradně pro vzdělávací účely, ke komunikaci se zaměstnanci školy a k získávání informací o průběhu studia. Škola si při využívání počítačové sítě vyhrazuje právo omezovat přístup k nežádoucím stránkám a serverům. V souladu se zákonem provádí škola monitorování provozu v síti a záznamy o logování uživatelů sítě.

3) Oprávněným uživatelem je žák, zákonný zástupce žáka a pracovník školy. Oprávněný uživatel se přihlašuje do sítě SPŠei a je plně odpovědný za veškerou činnost prováděnou jím osobně a kýmkoliv dalším, kdo použije (zneužije) jeho uživatelský účet (vyjma situace, kdy uživatel nemohl přes veškerou prokazatelně vynaloženou snahu tomuto zneužití zabránit).

4) Uživatel může na základě přihlašovacího jména a hesla sledovat výsledky průběžné klasifikace.

5) V případě ztráty nebo vyzrazení přihlašovacích údajů je každý uživatel povinen oznámit tuto skutečnost správci, ing. Janu Patschkovi, a to osobně (školní informační centrum) nebo pomocí e-mailového sdělení (j.patschka@spseiostrava.cz), pokud tak neučiní, nemůže škola nést odpovědnost za případné zneužití osobních údajů získaných třetí osobou.

6) Uživatel smí používat pouze přístupová práva, která mu byla správcem sítě přidělena a nesmí vyvíjet žádnou činnost směřující k obcházení tohoto ustanovení. Pokud uživatel jakýmkoliv způsobem získá přístupová práva, která mu správcem sítě nebyla přidělena (např. chybným nastavením bezpečnostních prvků sítě), je povinen tuto skutečnost neprodleně oznámit správci sítě. Takto, neoprávněně, získaná práva nesmí uživatel sítě použít.

III.

Uživatel školní počítačové sítě SPŠei **je povinen:**

1. Při komunikaci s uživateli jiných sítí je uživatel povinen dodržovat pravidla, která platí v těchto sítích.
2. Neprodleně ohlásit správci sítě jakékoliv závady ve funkčnosti prvků sítě.
3. Neprodleně nahlásit správci sítě jakékoliv zjištěné porušení těchto pravidel ze strany jiných uživatelů.
4. Po ukončení práce na počítači se neprodleně odhlásit ze sítě.

IV.

Uživatel školní počítačové sítě SPŠei zejména **nesmí:**

1. Provozovat jakoukoliv činnost v rozporu s platnými právními nebo etickými předpisy (např. zveřejňovat nebo šířit texty hanobící rasu, národ, přesvědčení, nebo skupinu obyvatel).
2. Umožnit používat svůj účet jiné osobě.
3. Používat jinou než vlastní identifikaci (vydávat se za někoho jiného, případně používat účet, který byl přidělen jiné osobě).
4. Měnit, případně se pokoušet o změnu systémové konfigurace počítačů, nebo jiných prvků sítě.
5. Poškozovat vybavení nebo funkčnost sítě.
6. Zbytečně zatěžovat síťové zdroje (přenosová kapacita síťových prvků, výpočetní výkon počítačů a diskový prostor serveru a pracovních stanic).
7. Využívat elektronických prostředků k obtěžování nebo zastrašování jiných uživatelů. Do této kategorie spadá i rozesílání řetězových dopisů či dopisů na náhodně vybrané síťové adresy.
8. Používat vulgárních a silně emotivních výrazů při komunikaci otevřené dalším účastníkům.
9. Navazovat komunikaci s náhodně vybranými účastníky jiných sítí.
10. Používat síť k získání neautorizovaného přístupu k neveřejným informačním zdrojům (i v majetku nebo správě jiných organizací).
11. Využívat nelegální programové vybavení a data, případně takovéto programy či data nabízet jiným.
12. Instalovat, nebo spouštět neautorizované programy bez předběžného souhlasu správce příslušné počítačové sítě.
13. Šířit nebo přechovávat destruktivní programy nebo data infikované počítačovými viry.
14. Provádět jakékoli akce, které vedou k narušení soukromí jiného uživatele, a to i v těch případech, kdy tento uživatel svá vlastní data explicitně nechrání.