Střední škola strojírenská a elektrotechnická Brno, příspěvková organizace

SŠ SE BRNO

Trnkova 2482/113, Brno, 628 00 Tel.: +420 544 422 811 Fax: +420 544 210 665 http://www.sssebrno.cz

Směrnice k bezpečnému provozu počítačové sítě na Střední škole technické a ekonomické Brno

Směrnice je vydána k zajištění bezpečnosti počítačové sítě na základě varování NÚKIB ze dne 20. dubna 2021

1. Všeobecné pokyny k používání výpočetní techniky a počítačové sítě

a. Počítačová síť a počítačové vybavení školy včetně mailových schránek slouží výhradně k výukovým a pracovním účelům.
b. Nelze na něm spouštět žádné aplikace, které neschválil správce počítačové sítě, a to bez ohledu na to, zda se instalují či nikoliv. Toto omezení se týká i mobilních telefonů, pokud se k síti připojují jakýmkoliv způsobem.
c. On-line aplikace lze spouštět za účelem výuky, pokud se jejich součásti a rozšíření neinstalují do technických zařízení školy
d. K síti školy nelze připojovat žádná soukromá zařízení, a to ani s vědomím správce sítě. Je-li to nezbytné – například u externích přednášejících – bude takové zařízení připojenou výhradně na segmentu sítě „počítačové učebny“ ve Výpočetním středisku na Domově mládeže.
e. Použití vlastních počítačů na Domovech mládeže pro tam ubytované je povoleno s tím, že za riziko bezpečnostních incidentů zodpovídá majitel takového zařízení, v případě neplnoletých žáků pak jejich zákonný zástupce.

2. Pokyny k používání výpočetní techniky

a. Všechny počítače, notebooky, tablety a podobná zařízení (dále jen „počítače“), která se připojují do sítě školy, musí mít zajištěnu ochranu odsouhlaseným antivirovým programem. Pokud uživatel zjistí, že zařízení není chráněno nebo antivirový program hlásí nedostatky ve své funkci, je povinností uživatele neprodleně průkazně informovat správu sítě. Správce sítě sjedná nápravu v nejkratším možném termínu.
b. Počítače a obdobná zařízení jsou pravidelně aktualizována, jejich systém je udržován pomocí vzdálené správy. Pokud je takové zařízení odneseno ze školy, například pro práci na home office, je nejméně jedenkrát měsíčně předáno ke kontrole správci sítě, který zařízení prověří antivirem a doinstaluje příslušné aktualizace. Zaměstnanec dohodne kontrolu tak, aby správa sítě zařízení zkontrolovala a mohla jej vrátit během téhož pracovního dne. Na vyzvání vedení školy, správy sítě nebo ICT koordinátora musí být zařízení kdykoliv k dispozici ve škole nejpozději do tří dnů od předání výzvy.
c. Pokud zaměstnanec používá flashdisk, ručí za jeho obsah a za to, že je takové zařízení zkontrolováno antivirem ve školní síti. Správa sítě ručí za správné nastavení antiviru a za to, že každé připojené zařízení automaticky projde kontrolou.
d. Při odchodu z pracoviště je zaměstnanec povinen zařízení řádně vypnout a v případě předpokládané delší nepřítomnosti, například dovolené, jej odpojí nejen od přívodu elektřiny, ale i od sítě školy.

3. Dodržování obecných bezpečnostních zásad

a. Zařízení školy ani síť školy nelze používat k soukromým účelům, hrám nebo zasílání soukromých mailů nebo k prohlížení stránek, nesloužících k pracovním účelům.
b. Žáci i zaměstnanci mají přísně zakázáno spouštět aplikace typu herních konzolí a dalších zábavních nebo loterijních aktivit.
c. Nelze zapůjčovat zařízení, určená pro učitele a provoz, žákům, ani s nimi nechávat žáky o samotě. Výjimku tvoří počítače v učebnách, a to pouze pod přímým dozorem vyučujícího a jen tehdy, pokud to vyžaduje výuka.
d. Je zakázáno půjčovat přístupové čipy dalším osobám za účelem tisku nebo skenování. Skeny dokumentů lze zaslat v rámci sítě školy kterémukoliv zaměstnanci přímo na tiskárně.
e. Všichni uživatelé techniky dbají na tzv. bezpečnostní triádu:
    i. **Důvěrnost** – vidím pouze ty údaje, které potřebuji ke své práci. Pokud vidím jiné údaje, než obvykle nebo naopak zjistím, že někdo jiný vidí údaje, které vidět nemá, došlo k porušení zásady Důvěrnosti. ***Příklad:*** *jako třídní učitel vidím docházku své třídy. Při práci v Edookitu ale náhle uvidím i docházku další třídy, kde třídním nejsem.* ***Jde o porušení zásady důvěrnosti*** *– toto ihned ohlásím správci Edookitu, zástupci ředitele nebo správě sítě.*
    ii. **Integrita:** údaje musí být úplně a správné. ***Příklad:*** *v počítači mám uloženy písemné práce, které zadávám v různých ročnících. Při rozdávání prací si všimnu, že v zadání pro druhý ročník jsou úlohy, vyřešené již v prvním ročníku. Po otevření souboru v počítači vidím, že byl změněn v době, kdy byl v kabinetu pouze kolega.* ***Jde o porušení zásady Integrity*** *– událost hlásím správci sítě a zástupci ředitele.*
    iii. **Dostupnost:** vždy mám dostupné ty zařízení a ta data, která mám mít a která potřebuji k práci. ***Příklad****: Na disku H: mám uložen soubor s docházkou, do kterého každý den zapisuji. V určitý den ale soubor nevidím a nemohu najít ani jiné osobní soubory. Jejich názvy jsou přepsány a ikony mají jiný tvar, než dosud.* ***Jde o porušení zásady Dostupnosti****. Okamžitě informuji správce sítě.*
f. Jakékoliv závady na technickém nebo programovém vybavení školy, neobvyklé chování používaných aplikací nebo souborů hlásí zaměstnanec průkazným způsobem (písemnou formou) správci sítě. V případě pochybností přivolá ICT koordinátora a hlášení provede on.

4. Komunikace vně školy

a. S žáky a jejich zákonnými zástupci komunikujeme zásadně pomocí řízeného prostředí přes systém EdooKit nebo školní Classroom. Mailovou komunikaci omezujeme na nezbytné minimum, neposíláme soubory ani přílohy ani je nepřijímáme.
b. Pokud nelze jinak a žák žádá například o přístup k Edookitu mailem, pak komunikujeme pouze přes adresy, uvedené v Edookitu v záložce Třídní kniha, Rodiče třídy/kurzu nebo záložku Žáci třídy.
c. S ostatními organizacemi a jednotlivci dbáme při mailové komunikaci zvýšené opatrnosti, pokud to lze, použijeme datovou schránku. Její užití schvaluje vedení školy.
d. V mailu máme vypnuté „náhledy". Pokud dostaneme pozvánku nebo reklamní sdělení, které nás zve na nějakou akci, otevíráme pouze odkazy, které ověříme po najetí myší kontrolou Stavového řádku v dolní části obrazovky.
e. Nikdy neposíláme své přihlašovací údaje ani údaje žáků na neověřenou adresu a nesdělujeme je třetím stranám, a to ani na telefonický dotaz. Požadavek na sdělení

takových informací nahlásíme ICT koordinátorovi nebo svému nadřízenému, a to i v případě, kdy jsme nic nepředali a ani tak nehodláme učinit.

5. Činnost v případě podezření na bezpečnostní hrozbu

a. V případě, že se počítač nechová standardně nebo vykazuje známky porušení některé z bezpečnostních zásad, informujeme ihned prokazatelnou formou (mailem) správu sítě.

b. Pokud máme podezření na virovou nákazu nebo se na počítači objeví výzva k zaplacení výkupného, okamžitě počítač vypojíme ze sítě školy, necháme jej zapnutý a informujeme správu sítě, ICT koordinátora a zástupce ředitele. Pokud si nejsme jisti, který kabel je síťový, požádáme o pomoc kolegy – učitele IKT, elektro nebo odborného výcviku.

c. Přístupové údaje do školních systémů jsou osobní a důvěrné. Pokud je někdo chce, informujete okamžitě správce systému nebo ICT koordinátora a oznámíte, od koho požadavek přišel.

Ing. Roman Moliš
Ředitel

V Brně, 26.04.2021