

Bezpečnostní pravidla pro využívání školní počítačové sítě a školní výpočetní techniky

Následující pravidla jsou závazná pro všechny zaměstnance **Střední školy gastronomie a služeb, Liberec, Dvorská 447/29, příspěvkové organizace** (dále jen **škola**) s platnou pracovní smlouvou, kteří jakýmkoli způsobem přistupují ke školní počítačové síti, mají zřízený uživatelský účet, který je k tomuto přístupu opravňuje nebo jakýmkoli jiným způsobem přistupují nebo nakládají s daty žáků a dalšími školními daty a elektronickými informacemi, dále jen **zaměstnanec**.

Bezpečnostní pravidla se vztahují na používání veškeré výpočetní techniky v majetku školy (počítače, notebooky, tablety, mobilní telefony a další) a také na všechna soukromá výpočetní zařízení (počítače, notebooky, tablety, mobilní telefony, chytré hodinky a další) v majetku zaměstnance, prostřednictvím kterých zaměstnanec přistupuje ke školní počítačové síti nebo školním datům a informacím v elektronické podobě, dále jen **zařízení**.

- 1) Školní uživatelský účet přidělený zaměstnanci správcem počítačové sítě slouží jako důvěryhodný identifikátor zaměstnance v rámci školní počítačové sítě. Veškerá činnost vykonaná pomocí tohoto uživatelského účtu je přisuzována vlastníku účtu bez ohledu na skutečnou osobu, která účet pro přístup použila.
- 2) Je zakázáno sdělovat přihlašovací údaje zaměstnance do školní počítačové sítě jiné osobě, a to i jinému zaměstnanci nebo rodinnému příslušníkovi. Přihlašovací údaje nesmí být fyzicky zapsané a uloženy na místě, kde by mohlo dojít ke zneužití údajů cizí osobou.
- 3) Zařízení v majetku školy mohou využívat pouze zaměstnanci školy s využitím školního uživatelského účtu. Je zakázáno umožnit přístup k zařízení osobě, která není zaměstnancem nebo žákem školy.
- 4) Zařízení v majetku školy svěřená do osobního využívání zaměstnanci může používat pouze zaměstnanec, který má zařízení zapsané v osobní kartě zaměstnance. Přístup k zařízení jiným zaměstnancem je možný pouze v případě, že se zaměstnanec přihlásí vlastním školním uživatelským účtem.
- 5) Je zakázáno jakýmkoli způsobem zasahovat do konfigurace zařízení v majetku školy (odinstalovat programy, měnit nastavení, vkládat skripty či jiné spustitelné soubory) bez schválení správce počítačové sítě.
- 6) Je zakázáno do zařízení v majetku školy instalovat jakýkoli software bez schválení správce počítačové sítě.
- 7) Je zakázáno jakýmkoli způsobem manipulovat s hardware a kabeláží zařízení (mimo odpojování a připojování myši a klávesnice, či jiné drobné opravy) bez schválení správce počítačové sítě.
- 8) Je zakázáno používat zařízení v majetku školy k účelům, které nesouvisí s pracovní náplní zaměstnance.
- 9) Zaměstnanec je odpovědný za veškerou činnost v rámci školní počítačové sítě, která byla provedena jeho uživatelským účtem a za případné bezpečnostní incidenty, které prostřednictvím jeho účtu vzniknou.
- 10) Zaměstnanec je povinen dodržovat obecná bezpečnostní pravidla pro bezpečný pohyb na veřejném internetu a pravidla prevence kybernetických hrozeb.
- 11) Každé zařízení v majetku zaměstnance, které zaměstnanec připojí ke školní počítačové síti nebo v něm použije školní přihlašovací údaje, musí být zabezpečeno. Zaměstnanec odpovídá za veškeré bezpečnostní incidenty způsobené tímto zařízením.
- 12) Každý bezpečnostní incident bude vyšetřen a evidován správcem počítačové sítě. Bezpečnostním incidentem se rozumí jakékoliv narušení bezpečnosti školní sítě, porušení těchto pravidel, únik citlivých informací, neoprávněný přístup k uživatelskému účtu, neoprávněný zásah do školních systémů, ztráta nebo poškození školních dat a další, a to i ve stádiu pokusu.
- 13) Každé podezření z narušení bezpečnosti školní počítačové sítě je zaměstnanec povinen nahlásit správci počítačové sítě, a to bez zbytečného odkladu i mimo pracovní dobu jakýmkoli dostupným komunikačním prostředkem.
- 14) Veškeré výjimky z výše uvedených pravidel musí být schváleny a provedeny správcem počítačové sítě.
- 15) Škola si vyhrazuje právo upravit nebo doplnit tato pravidla. Aktuální znění bezpečnostních pravidel bude vždy přístupné na zaměstnaneckém portále (<https://zamestnanec.sos-gs.cz>).

Porušení výše uvedených pravidel bude prověřeno správcem počítačové sítě a vedením školy. Porušení výše uvedených pravidel znamená porušení pracovních povinností zaměstnance s pracovní právními důsledky s tím spojenými dle závažnosti incidentu.

Každý zaměstnanec svým podpisem stvrdí, že byl s výše uvedenými pravidly srozuměn a rozumí jim.

Podepsané dokumenty jsou uloženy u vedení školy.

Platnost dokumentu: od 01. 08. 2024