

Základní škola Hlučín, Hornická 7, okres Opava, příspěvková organizace	
Řád informační a kybernetické bezpečnosti	
Č.j.: ZšHIHo/0361/2024	Účinnost od: 19. 04. 2024
Spisový znak: 3.1.1.	Skartační znak: A5
Změny: 19. 04. 2024	

## Vnitřní řád informační a kybernetické bezpečnosti

### 1. Přístupová kontrola:

Přístup k ICT ve správě školy je povolen pouze autorizovaným uživatelům, a to pod dohledem vyučujícího, není-li stanoveno jiným rozhodnutím vedení školy jinak.

Každý uživatel se musí při užívání ICT ve správě školy přihlásit pomocí svého unikátního uživatelského jména a hesla.

Není tolerováno sdílení přihlašovacích údajů.

### 2. Fyzická bezpečnost:

Učebna, ve které se nachází ICT ve správě školy, musí být uzamčena mimo provozní hodiny.

Veškerá zařízení v učebně musí být zajištěna proti krádeži.

### 3. Ochrana dat:

Veškerá citlivá data musí být ukládána na chráněných síťových serverech. Není přípustné užívat servery třetích stran. Výjimku tvoří servery pod správou a vlastnictvím zřizovatele naší organizace.

Žádná citlivá data nesmí být uložena na osobních zařízeních.

Osobní zařízení či zařízení ve vlastnictví a správě jiných stran je zakázáno připojovat do sítě či k zařízením ICT ve správě školy. Výjimku z tohoto nařízení tvoří připojení k WiFi síti ZSHORNICKA a WiFi iPad Hornicka, avšak pouze za předpokladu, že takto připojené zařízení nebude navedeno do domény školy jakýmkoli způsobem.

Uživatelé musí respektovat autorská práva a dodržovat pravidla a licenční ujednání ohledně používání softwaru a dalšího obsahu.

### 4. Bezpečnostní aktualizace:

Veškerý software v učebně musí být pravidelně aktualizován na nejnovější verze k zajištění bezpečnosti a stability. Užívání nepodporovaného a zastaralého software-u je striktně zakázáno.

Výjimku z tohoto pravidla může udělit jen vedení školy po konzultaci s ICT metodiky a koordinátory a správcem sítě.

## **5. Síťová bezpečnost:**

Používání osobních zařízení v síti učebny se řídí dle odstavce 3 tohoto dokumentu a je povoleno pouze v případech, kdy jsou splněny všechny podmínky předchozí, a navíc je toto zařízení schváleno k užití správcem sítě či ICT metodikem a koordinátorem k danému účelu.

Každý uživatel je povinen dodržovat pravidla sítě týkající se používání internetu a komunikace.

## **6. Zálohování dat:**

Důležitá data musí být pravidelně zálohována a kopie musí být uloženy na bezpečném místě dle GDPR. Za zálohu dat zodpovídá pracovník, který jako poslední s daty nakládal, měnil je a upravoval.

## **7. Vyřazení zařízení:**

Před vyřazením starých zařízení musí být zabezpečeny veškeré citlivé údaje a paměťová zařízení musí být zničena nebo smazána nenávratným způsobem.

## **8. Nahlášení bezpečnostních incidentů:**

Každý podezřelý bezpečnostní incident musí být okamžitě nahlášen správci sítě, ICT metodikovi a koordinátorovi nebo vedení školy.

## **9. Užívání školních komunikačních technologií**

Je zakázáno školními komunikačními prostředky jakýmkoli způsobem sdílet data, která by mohla být označena jako závadová. Závadová data jsou taková, která porušují autorská práva a jiné další právní předpisy (ohrožují mravní výchovu mládeže, mohla by být zneužita ke kyberútoku či kyberšikaně, mají urážlivý obsah, obsahují zakázanou symboliku apod.).

## **10. Školení uživatelů:**

Všichni uživatelé jsou povinni absolvovat školení týkající se bezpečnosti informačních technologií a zavádění nových ICT technologií do organizace.

Tento vnitřní řád je pravidelně aktualizován a přizpůsobován v souladu s aktuálními bezpečnostními standardy a potřebami organizace a každý člen organizace je povinen aktivně vyhledávat a seznamovat se s aktuálním zněním.

V Hlučín dne 19. 4. 2024

Mgr. Martin Franek  
ředitel školy