CYBERSEC
EDUCHECK

MANUÁL
PRO STŘEDNÍ ŠKOLY

PODPORA UDRŽENÍ ODPOVÍDAJÍCÍ ÚROVNĚ INFORMAČNÍ BEZPEČNOSTI ŠKOLY A PODPORA VZDĚLÁVÁNÍ A INFORMOVANOSTI V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

Připravil:
Mateusz Pękala

PROJEKT Č. 2023-2-PL01-KA210-VET-000176822

Spolufinancováno Evropskou unií

VŮDCE:
Research Institute Europe | Coventry University

PARTNEŘI:
KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

Obsah

Pro koho?

Tento manuál je pro vás, pokud:

→ Jste ředitelem nebo zástupcem ředitele střední školy a zodpovídáte za informační bezpečnost ve své instituci

→ Zaznamenáváte rostoucí potřebu zavádět mezi studenty a zaměstnance efektivní vzdělávací aktivity v oblasti kybernetické bezpečnosti

→ Chcete vytvořit pravidla pro používání technologií, které pomohou předcházet kyberšikaně, dezinformacím a dalším digitálním hrozbám

→ Hledáte praktické tipy, jak budovat povědomí o kybernetických hrozbách ve školním prostředí, jak zapojit studenty i zaměstnance

→ Chcete, aby vaše škola byla příkladem dobré praxe v řízení digitální bezpečnosti a ochrany dat

Tento manuál byl vypracován jako komplexní průvodce, který má pomoci ředitelům škol při vytváření rámců vzdělávání v oblasti kyberbezpečnosti a řízení informační bezpečnosti. Reaguje tak na výzvy spojené s vedením školy a jejím cílem je předcházet mimo jiné neetickému, nejistému a rizikovému chování mezi mládeží využívající technologie.

Co najdete v manuálu?

Manuál poskytuje nástroje, které vám pomohou efektivně zavést program informační bezpečnosti ve škole:

- **Definice rolí a odpovědností** – naučíte se, jak jasně přidělit úkoly související s informační bezpečností všem zaměstnancům, od učitelů po vedení.
- **Zavedení bezpečnostních politik** – naučíte se, jak implementovat Systém řízení informační bezpečnosti a Politiku bezpečnosti informací, což zajistí ochranu dat ve vaší škole.
- **Program budování povědomí** – najdete návrh vzdělávacích aktivit, které pomohou zvýšit povědomí o kybernetických hrozbách mezi studenty a zaměstnanci.

V přílohách manuálu najdete šablony dokumentů. Tyto nástroje vám pomohou přizpůsobit zásady bezpečnosti specifikům vaší školy a vybudovat pevné základy digitální bezpečnosti. Přečtěte si manuál a využijte šablony k efektivnímu řízení bezpečnosti informací ve vaší instituci.

Definice rolí a odpovědností

Ve školách, kde jsou omezené zdroje a prioritou je realizace výukového programu a péče o studenty, je důležité jasně určit role a odpovědnosti za informační bezpečnost. To je klíčový první krok k budování Systému řízení informační bezpečnosti.

Každý člen školní komunity, od učitelů, vychovatelů a pedagogů po psychology a vedení školy, má svou roli v péči o kybernetickou bezpečnost. Určení vhodných rolí a povinností zajišťuje, že činnosti související s informační bezpečností budou efektivně vykonávány na všech úrovních školy a stanovená pravidla budou dodržována.

Pro usnadnění tohoto procesu najdete v příloze šablonu „Role a povinnosti v SŘIB" (dokument 02) a hlavní dokument „Politika bezpečnosti informací" (dokument 01). Oba dokumenty pomohou při efektivním řízení bezpečnosti informací ve vaší instituci.

Zavedení systému řízení informační bezpečnosti

Jedním z klíčových prvků Systému řízení informační bezpečnosti (SŘIB) ve škole je vytvoření Školícího programu, který buduje a udržuje povědomí o kybernetické bezpečnosti. Přirozeně se vzdělávání ve škole zaměřuje na předávání nových znalostí, ale stejně důležité je pravidelné připomínání platných pravidel, jako jsou zásady bezpečnosti a používání silných hesel. V tomto kontextu by škola měla zavést mechanismy, které zajistí pravidelné připomínání a upevňování těchto zásad.

Je důležité mít na paměti, že studenti nemají stejné povinnosti jako dospělí zaměstnanci, a proto by program budování povědomí měl být přizpůsoben specifikům školy. Tento program zahrnuje celou školní komunitu – zaměstnance i studenty – společně bojující proti kybernetickým hrozbám.

Pro realizaci tohoto cíle doporučujeme šablonu „Program budování povědomí v oblasti kybernetické bezpečnosti“ (dokument 04). Tento dokument je potřeba přizpůsobit specifikům konkrétní školy – ne každá škola má přístup k takovým zdrojům, jako jsou přednášky policie, externí školení nebo podpora rodičů pracujících v IT oboru. Pokud však tyto možnosti existují, je vhodné je zahrnout do plánu.

Šablonu „Program budování povědomí v oblasti kybernetické bezpečnosti“ (dokument 04) spolu s instrukcemi pro vyplnění najdete v příloze manuálu.

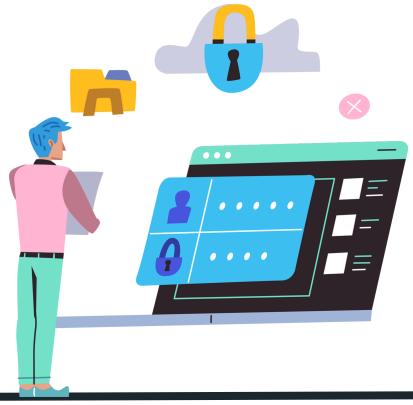
Program budování povědomí o kybernetické bezpečnosti ve škole

Jedním z klíčových prvků **Systému řízení informační bezpečnosti** (SŘIB) ve škole je vytvoření Školícího programu, který buduje a udržuje povědomí o kybernetické bezpečnosti. Přirozeně se vzdělávání ve škole zaměřuje na předávání nových znalostí, ale stejně důležité je pravidelné připomínání platných pravidel, jako jsou zásady bezpečnosti a používání silných hesel. V tomto kontextu by škola měla zavést mechanismy, které zajistí pravidelné připomínání a upevňování těchto zásad.

Je důležité mít na paměti, že žáci nemají stejné povinnosti jako dospělí zaměstnanci, a proto by program budování povědomí měl být přizpůsoben specifikům školy. Tento program zahrnuje celou školní komunitu – zaměstnance i studenty – společně stojící na jedné straně v boji proti kybernetickým hrozbám.

Pro realizaci tohoto cíle doporučujeme šablonu **„Program budování povědomí v oblasti kybernetické bezpečnosti“** (dokument 04). Tento dokument je třeba přizpůsobit specifikům konkrétní školy – ne každá škola má přístup k takovým zdrojům, jako jsou přednášky policie, externí školení nebo podpora rodičů pracujících v IT oboru. Pokud však tyto možnosti existují, je vhodné je zahrnout do plánu.

Šablonu **„Program budování povědomí v oblasti kybernetické bezpečnosti“** (dokument 04) spolu s instrukcemi pro vyplnění najdete v příloze Manuál.



Seznam příloh

1. Politika informační bezpečnosti (PIB)

Dokument stanovující obecné zásady a cíle bezpečnosti informací ve škole.

2. Role a povinnosti v SŘIB

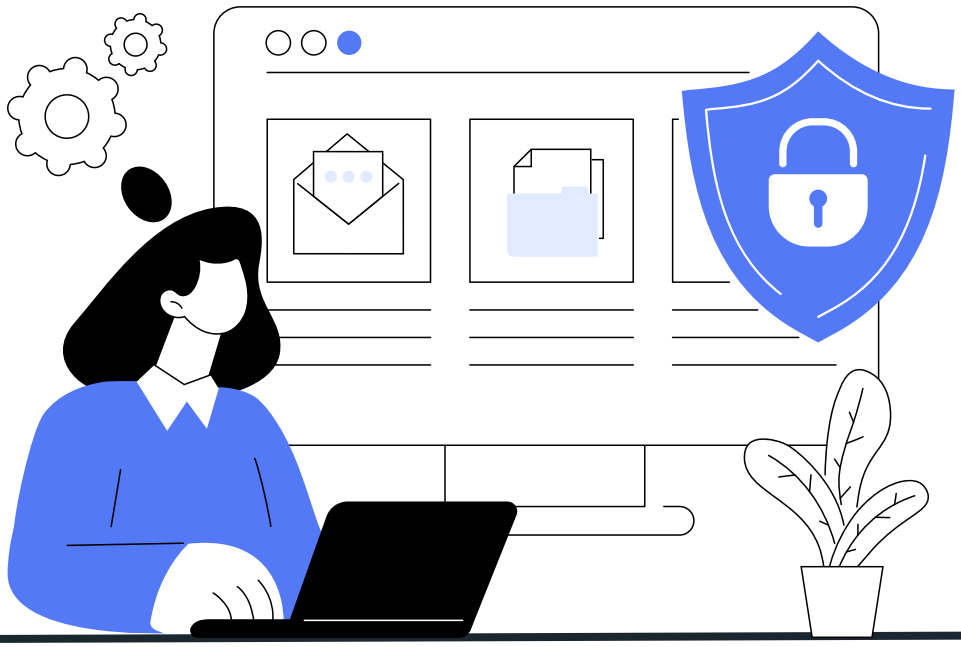
Šablona dokumentu definující odpovědnosti a úkoly školního personálu (učitelů, administrativy, vedení) v oblasti informační bezpečnosti.

3. Zásady bezpečnosti informací

Pravidla týkající se využívání IT zdrojů, mobilních zařízení a dodržování bezpečnostních politik.

4. Program budování povědomí v oblasti kybernetické bezpečnosti

Šablona vzdělávacího programu pro studenty a zaměstnance, který podporuje vzdělávání a udržování povědomí o kybernetických hrozbách.



1. Zásady informační bezpečnosti (PIB)

Vlastnosti dokumentu

Jméno	**Zásady informační bezpečnosti**
Schválení a dohled	Ředitel
Recenze	Pracovník pro informační bezpečnost školy
Frekvence kontrol	Jednou ročně nebo po jakékoli významné změně v procesu
Místo uložení	Intranet / vyhrazená složka na síťovém disku

Historie verzí

Verze	Data	Autor	Popis změn
0,1	01.10.2024	Univerzita v Coventry	Příprava návrhu šablony

Obsah

Zavedení

Odpovědnost za informační bezpečnost mají všichni zaměstnanci, dočasní a externí pracovníci (dodavatelé) a vedení školy.

Studenti jsou zodpovědní za dodržování pokynů týkajících se informační bezpečnosti, které jim poskytuje vedení školy a učitelé. Škola provádí vzdělávací činnost způsobem, který chrání zaměstnance, dodavatele, žáky a rodiče před nežádoucími bezpečnostními incidenty, jež ovlivňují důvěrnost, integritu a/nebo dostupnost zpracovávaných informací.

Cílem tohoto dokumentu je zavést Systém řízení informační bezpečnosti (SŘIB) ve škole, včetně definování odpovědností za jeho fungování a stanovení rámců pro stanovení konkrétních cílů v oblasti bezpečnosti. Vedení školy zajišťuje, že informační bezpečnost je důležitým aspektem činnosti školy, a deklaruje plné zapojení do zavádění a řízení SŘIB, mimo jiné prostřednictvím zajištění odpovídajících organizačních a finančních zdrojů.

Zásady informační bezpečnosti

• Cíl

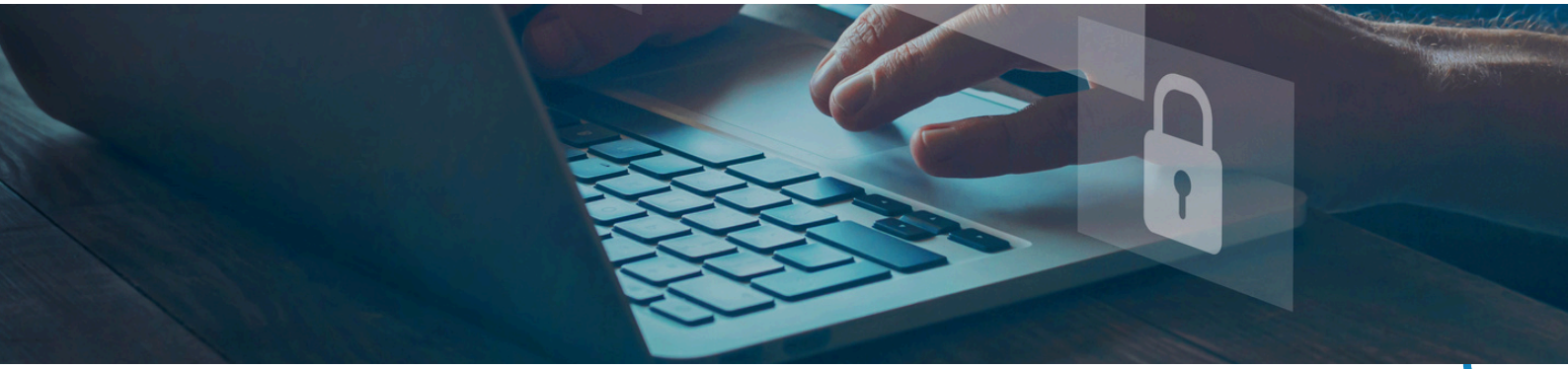
Cílem SŘIB je zajištění bezpečnosti informací v souladu s identifikovanými potřebami a očekáváními vedení, zaměstnanců, žáků, rodičů a dalších zainteresovaných stran školy.

• Podporované cíle organizace

SŘIB podporuje následující cíle organizace:

- Prokazování závazku a podpory vedení školy vůči bezpečnosti informací.
- Zavedení odpovídajících zabezpečení na základě identifikovaných rizik.
- Soulad s interními a externími závazky.
- Soulad s požadavky dozorových orgánů školy a smluvními závazky v oblasti bezpečnosti informací.
- Soulad se závaznými požadavky na ochranu soukromí dat, včetně požadavků GDPR.

Tato politika informační bezpečnosti je podporována a doplňována dalšími politikami, postupy a ostatní dokumentací SŘIB, včetně politik souvisejících s GDPR.



- **Rozsah SŘIB**

Tato politika se vztahuje na všechny procesy a informace spravované školou, včetně cloudových služeb, softwaru, zařízení, personálu a prostor.

- **Role a povinnosti v SŘIB**

S ohledem na nutnost integrace procesů souvisejících s informační bezpečností do běžné činnosti školy a také provozní a výkazní povinnosti, vedení školy stanoví odpovídající strukturu rolí a povinností, přičemž bere v úvahu nutnost přidělení odpovědnosti za celkové fungování Systému řízení informační bezpečnosti.

Školní úředník pro informační bezpečnost ve škole je odpovědný za udržování Politiky informační bezpečnosti, podporu jejích cílů a poradenství ohledně její implementace.

Personál (učitelé, vychovatelé, pedagogové) bude odpovědný za implementaci a provádění ustanovení Politiky informační bezpečnosti a souvisejících dokumentů ve svých oblastech.

Studenti musí být informováni o svých povinnostech v oblasti informační bezpečnosti.

2. Role a odpovědnosti v ISMS

Vlastnosti dokumentu

Jméno	Role a odpovědnosti v SŘIB
Schválení a dohled	Ředitel
Recenze	Pracovník pro informační bezpečnost školy
Frekvence kontrol	Jednou ročně nebo po jakékoli významné změně v procesu
Místo uložení	Intranet / vyhrazená složka na síťovém disku

Historie verzí

Verze	Data	Autor	Popis změn
0,1	01.10.2024	Univerzita v Coventry	Příprava návrhu šablony

Obsah

CÍL

Cílem dokumentu je definovat role a povinnosti, které jsou důležité pro efektivní fungování Systému řízení informační bezpečnosti (SŘIB).

Role a povinnosti v SŘIB

Škola určila role a odpovědnosti v rámci SŘIB.
Role v SŘIB mohou být kombinovány a vykonávány stejnými lidmi podle možností školy.

- **Ředitel**

Ředitel školy poskytuje vizi, podporuje implementaci a fungování SŘIB a zajišťuje obecné směrnice, směr a podporu pro fungování Systému řízení informační bezpečnosti ve škole.

Povinnosti ředitele školy zahrnují:

- Schválení cílů a rozsahu SŘIB s ohledem na cíle školy a právní požadavky,
- Určení rolí a schvalování organizačních změn souvisejících se SŘIB,
- Schválení Politiky informační bezpečnosti,
- Schvalování dokumentů SŘIB vycházejících z Politiky informační bezpečnosti,
- Schvalování přijatelné úrovně rizika, výsledků analýzy rizik a plánů řešení rizik v procesech pokrytých SŘIB,
- Schválení rozpočtu souvisejícího se SŘIB,
- Schvalování výsledků auditů a přezkumů SŘIB,
- Rozhodování v rámci krizového řízení.

- **Školní úředník pro informační bezpečnost**

Školní úředník pro informační bezpečnost je zodpovědný za fungování SŘIB, přípravu směrnic a dohled nad bezpečností informací.

Mezi povinnosti důstojníka patří:

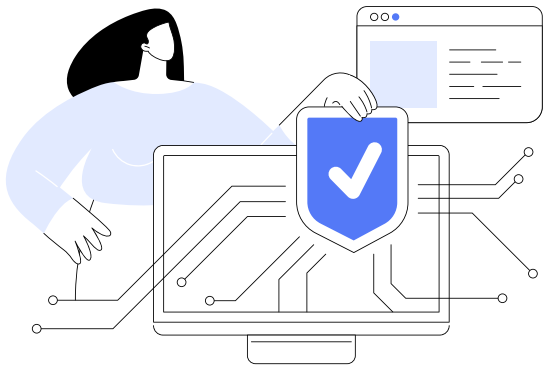
1. Zavádění změn a dohled nad konzistencí dokumentace SŘIB a provádění jejích pravidelných přezkumů a aktualizací,
2. Zvyšování povědomí zaměstnanců a studentů o otázkách bezpečnosti informací, zejména dohled nad Programem budování povědomí v oblasti kybernetické bezpečnosti ve škole,
3. Implementace a dohled nad dodržováním zásad a mechanismů souvisejících s bezpečností informací,
4. Hodnocení účinnosti plnění požadavků vyplývajících z předpisů o bezpečnosti informací.

- **Inspektor ochrany osobních údajů (IOD)**

Školy, které již disponují dokumentací v oblasti ochrany osobních údajů (GDPR), mohou na tyto záznamy odkazovat a nemusí znovu definovat povinnosti IOD. Je důležité, aby dokumentace SŘIB a politiky týkající se ochrany osobních údajů byly integrovány. Ve skutečnosti je shoda s GDPR jedním z cílů SŘIB.

IOD (Inspektor ochrany osobních údajů) pomáhá personálu školy ve všech záležitostech týkajících se ochrany osobních údajů. Povinnosti IOD zahrnují:

- Informování a poskytování poradenství vedení školy a zaměstnancům o jejich povinnostech vyplývajících z legislativy o ochraně osobních údajů,
- Monitorování souladu se všemi předpisy týkajícími se ochrany údajů, včetně auditů, aktivit zaměřených na zvyšování povědomí a školení zaměstnanců zapojených do zpracování dat,
- Poskytování poradenství při provádění posouzení vlivu na ochranu údajů (DPIA) a sledování jeho účinnosti,
- Působení jako kontaktní místo pro žádosti jednotlivců týkající se zpracování jejich osobních údajů a uplatňování jejich práv,
- Spolupráce s orgány ochrany údajů a fungování jako kontaktní bod pro tyto orgány v otázkách souvisejících se zpracováním osobních údajů,
- Podpora činností spojených s údržbou a zlepšováním SŘIB v oblasti ochrany osobních údajů,
- Podpora při výběru ochranných opatření přiměřených množství a rozsahu zpracování osobních údajů,
- Podpora projektových prací na systémech zpracovávajících osobní údaje,
- Klasifikace operací zpracování osobních údajů podle množství, typu a účelu zpracování,
- Vedení evidence operací zpracování osobních údajů.



- **Učitel/zaměstnanec**

Všichni zaměstnanci, kteří mají přístup k informačním zdrojům školy, včetně zaměstnanců, dodavatelů, stážistů a externích poskytovatelů služeb, mají povinnost:

1. Dodržovat Politiku informační bezpečnosti a zásady informační bezpečnosti stanovené v dalších souvisejících dokumentech.
2. Dodržovat Politiku ochrany osobních údajů a související předpisy.
3. Hlásit incidenty související s bezpečností informací.
4. Účastnit se školení v oblasti bezpečnosti informací.

- **Student**

Všichni studenti, kteří mají přístup k informačním zdrojům školy v rozsahu požadovaném jejich třídou,

mají povinnost:

1. Dodržovat Politiku informační bezpečnosti a zásady bezpečnosti informací stanovené v dalších souvisejících dokumentech.
2. Dodržovat Politiku ochrany osobních údajů a související předpisy.
3. Hlásit incidenty související s informační bezpečností.
4. Účastnit se školení v oblasti informační bezpečnosti.
5. Poslouchat pokyny učitelů a ostatního pedagogického personálu ohledně používání elektronických zařízení a internetu na území školy.

3. Pravidla informační bezpečnosti

Vlastnosti dokumentu

Jméno	**Pravidla informační bezpečnosti**
Schválení a dohled	Ředitel
Recenze	Pracovník pro informační bezpečnost školy
Frekvence kontrol	Jednou ročně nebo po jakékoli významné změně v procesu
Místo uložení	Intranet / vyhrazená složka na síťovém disku

Historie verzí

Verze	Data	Autor	Popis změn
0,1	01.10.2024	Univerzita v Coventry	Příprava návrhu šablony

Obsah

Prosím, mějte na paměti, že dokument musí být přizpůsoben kontextu školy. Pokud považujete některé záznamy za nerealizovatelné, je samozřejmě vhodné se zamyslet, proč tomu tak je, a následně je odstranit/upravit/nahradit jiným opatřením, které kompenzuje riziko.

Obecné směrnice

1. Uživatel znamená každou osobu (zaměstnance školy a studenta) využívající informační zdroje školy, včetně internetu.
2. Škola poskytuje zaměstnanci IT vybavení jako nástroj umožňující vykonávat práci (úkoly) pro školu.
3. Uživatel nese odpovědnost za svěřené zařízení a software a za způsob jejich používání.
4. Uživatel nese finanční a právní důsledky za držení nelegálního softwaru na zařízení, které mu bylo svěřeno školou.
5. Přísně je zakázáno testovat a/nebo narušovat zabezpečení zařízení a teleinformačního systému poskytovaného školou.
6. Zařízení svěřené školou nesmí být zpřístupňováno neoprávněným osobám.
7. Je zakázáno provádět jakékoli změny v konfiguraci dodaných zařízení nebo softwaru, pokud změna nebyla schválena Školním úředníkem pro informační bezpečnost. To se týká zejména změn nastavení souvisejících se zabezpečením.
8. Každý uživatel je povinen se seznámit se všemi předpisy, pokyny a interními postupy, které zavádí vedení školy.

Práce na dálku

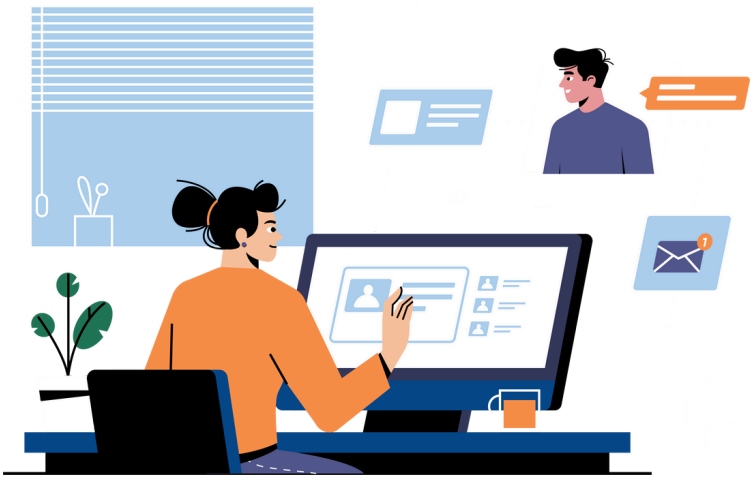
Poznámka: Toto se týká vybavení zakoupeného školou, nikoli například soukromého notebooku učitele používaného k práci. Tato situace se bude vztahovat k bodu o práci na soukromých zařízeních nebo BYOD, což znamená „Bring Your Own Device“.

1. Vynášení svěřeného mobilního zařízení mimo prostory školy musí být odůvodněno povinnostmi vykonávanými uživatelem.

2. Uživatel mobilního zařízení je povinen ho chránit. Je třeba se vyhnout rizikovému chování, které může zahrnovat mimo jiné:
- ponechání zařízení bez dozoru (v autě, hotelových pokojích apod.),
- ponechání tašky s notebookem bez dozoru,
- neodhlášení uživatele v případě dočasné nepřítomnosti nebo nečinnosti,
- umístění monitorů tak, aby bylo možné nahlížet na obsah obrazovky neoprávněným osobám.

3. V případě ztráty svěřeného mobilního zařízení používaného mimo školu by měl uživatel tuto skutečnost neprodleně nahlásit Školnímu úředníkovi pro informační bezpečnost, a v případě krádeže navíc tuto skutečnost ohlásit policii.

.



Bezpečná správa přihlašovacích údajů a hesel

Informace o identifikátorech by měly být odstraněny pro školy, které je nepoužívají. Politika hesel by měla být v souladu s aktuálními směrnicemi v této oblasti. Často uplatňovaná politika časté změny hesel, například každých 30 dní, a používání krátkých hesel o délce pouze 8 znaků není dobrým řešením.

1. Uživatel nese odpovědnost za všechny činnosti prováděné s použitím jeho identifikátoru a hesla.
2. Hesla uživatelů a jiná ověřovací data podléhají speciální ochraně.
3. Každý uživatel, který má přístup do informačního systému školy, je povinen:
   - Uchovávat všechna svá hesla a jiné autentizační údaje v tajnosti.
   - Neprodleně změnit heslo při podezření nebo skutečném úniku hesla.
   - Používat hesla o minimální délce 12 znaků, která obsahují velká a malá písmena, číslice a/nebo speciální znaky.
   - Doporučuje se používat dvoufaktorové ověřování, kde je to možné.
4. Hesla nesmí být zapisována žádným jednoznačným způsobem (např. textové soubory, poznámkový blok atd.).
5. Je povoleno používat schválený systém určený pro bezpečné ukládání hesel (správce hesel).
6. Je zakázáno přihlašovat se do systému pomocí přihlašovacích údajů jiného uživatele.
7. Uživatel je povinen zablokovat počítač, který není aktuálně používán, aby předešel neautorizovanému přístupu, čímž vynutí zablokování obrazovky chráněné heslem (zásada čisté obrazovky).

Používání internetu, e-mailu, internetových komunikátorů

1. **Pokud používáte internet ve škole, musíte se bezpodmínečně vyhnout rizikovému chování, včetně:**
   - Prohlížení webových stránek obsahujících nežádoucí obsah, zejména stránek pornografických, rasistických, podněcujících k nenávisti, propagujících sekty, hazardních nebo jakýmkoli způsobem urážejících pocity ostatních či porušujících obecně uznávané zásady společenského soužití.
   - Prohlížení webových stránek obsahujících jakýkoli druh škodlivého softwaru (např. malware, exploity apod.).
   - Prohlížení webových stránek obsahujících kódy umožňující prolomení nebo obejití ochrany autorských práv.
   - Stahování, instalace, ukládání nebo šíření softwaru z internetu, který není školou autorizován.
2. Je zakázáno přistupovat k webovým stránkám, které jsou využívány k nelegální distribuci obsahu (děl) porušujícího předpisy o ochraně autorských práv.
3. E-mailové schránky s adresou poskytovanou školou mohou být používány výhradně pro korespondenci související s činností školy.
4. Je zakázáno přeposílat poštu na schránky, které nejsou spojeny se školou, zejména soukromé. Tento bod znamená, že například učitel si nemůže posílat materiály na soukromou e-mailovou schránku – škola by měla zvážit, zda si může v praxi dovolit toto opatření zakázat.

Toto ustanovení znamená, že například učitel nemůže posílat materiály do své soukromé schránky – škola by měla zvážit, zda si může v praxi dovolit toto opatření zakázat.

5. Při odesílání příloh, které obsahují školní tajemství nebo jsou chráněny příslušnými právními předpisy (např. obsahující osobní údaje), musí být tato příloha zašifrována heslem splňujícím požadavky uvedené ve třetím bodě zásad. Heslo nesmí být zasláno stejným komunikačním kanálem jako zpráva.

Požadavky na používání zařízení soukromých uživatelů pro práci nebo studium ve škole (BYOD)

1. Je povoleno používat pouze zařízení a systémy podporované výrobcem (pro které jsou poskytovány bezpečnostní opravy).
2. V případě:
   - ztráty soukromého zařízení (např. v důsledku ztráty nebo krádeže) sloužícího k zpracování důvěrných dat školy,
   - podezření na únik důvěrných dat školy, uživatel neprodleně informuje o takové události Školního úředníka pro informační bezpečnost,

uživatel o vzniku takové události neprodleně informuje pracovníka pro informační bezpečnost školy.

3. V případě ztráty soukromého zařízení uživatele, jeho prodeje nebo ukončení spolupráce se školou uživatel souhlasí s tím, že škola může odstranit vybraná nebo všechna (v závislosti na technických možnostech) data patřící škole.

4. V případě ukončení spolupráce se školou, přerušení používání zařízení pro účely BYOD nebo likvidace soukromého zařízení sloužícího ke zpracování školních dat, se uživatel zavazuje kontaktovat Školního úředníka pro informační bezpečnost za účelem trvalého odstranění dat, která jsou majetkem školy.

Zabezpečení informací

1. Povinností uživatele je podniknout kroky k ochraně informací, které zpracovává nebo vytváří. Uživatel má následující možnosti zabezpečení informací (souborů):
   - Doporučuje se ukládat data do složky určené školním úředníkem pro informační bezpečnost a používat řešení pro ukládání dat schválené školou.
   - pomocí řešení pro ukládání dat schválené školou.

2. Jiné způsoby ukládání dat školy jsou zakázány.
3. Je zakázáno zpracovávat informace na externích úložných zařízeních (např. USB disky, přenosné disky), které nejsou majetkem školy a nebyly kryptograficky zabezpečeny.
4. Je zakázáno zpřístupňovat informace (data, soubory) patřící škole neoprávněným osobám.

Bezpečné pracovní prostředí

1. Aby se snížilo riziko neoprávněného přístupu, ztráty nebo poškození informací během pracovní doby i mimo ni, je uživatel povinen:

- Dodržovat zásadu nezanechávat otevřené a nezabezpečené dveře umožňující přístup do místnosti,
- Zajistit ochranu přístupové karty a v případě její ztráty okamžitě informovat o této skutečnosti ochranu objektu a Školního úředníka pro informační bezpečnost,
- Uchovávat papírové dokumenty a vyměnitelné úložné média v odpovídajících zabezpečených kancelářských skříních,
- Po ukončení práce uspořádat své pracovní místo, aby se zabránilo neautorizovanému přístupu k dokumentům obsahujícím chráněné informace (zásada „čistého stolu“).

Hlášení incidentů a událostí

1. **V případě zjištění události, která může být důkazem nebo příznakem porušení bezpečnosti, nesprávné funkce softwaru, chyby nebo selhání systému, by měl uživatel:**

- Přestat pracovat na počítači
- Neprodleně informovat Školního úředníka pro informační bezpečnost / IT pracovníka a/nebo přímého nadřízeného / vedení školy o události, který provede analýzu, zda je nutné odpojit počítač od sítě.

2. Hlášení lze provést:

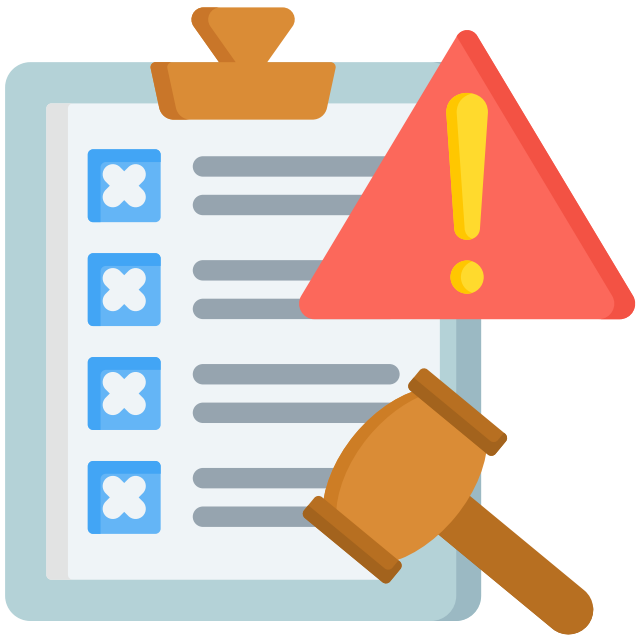
- E-mailem na adresu školy
- Osobně Školnímu úředníkovi pro informační bezpečnost / IT pracovníkovi a/nebo přímému nadřízenému / vedení školy.

3. Ohlášení by mělo obsahovat

- Označení uživatele nebo oblasti, která byla svědkem/ účastníkem události,
- Označení nebo identifikaci systému, kterého se incident týká,
- Přibližný čas výskytu incidentu,
- Popis okolností a míst, kde k události došlo, a symptom/popis události.i.

Disciplinární sankce

1. Nedodržování zásad uvedených v těchto pravidlech může vést k příslušným disciplinárním sankcím.
2. Pokud porušení stanovených zásad povede k podezření na porušení zákona, vedení školy předá veškeré důkazy orgánům činným v trestním řízení k dalšímu řízení.
3. Každý uživatel je povinen průběžně dodržovat všechny předpisy, pokyny a interní postupy zaváděné vedením školy. Všechny předpisy jsou uchovávány na disku Google/OneDrive/Sharepoint/síťovém disku.
4. V případě zavedení nového dokumentu (předpis, postup, pokyny apod.) je Školní úředník pro informační bezpečnost a/nebo přímý nadřízený odpovědný za zajištění efektivního způsobu komunikace těchto předpisů uživatelům.
5. Neznalost aktuálních bezpečnostních předpisů nebude důvodem k posuzování neviny uživatele a může vést k disciplinárnímu řízení.



4. Program budování povědomí o kybernetické bezpečnosti ve škole

Vlastnosti dokumentu

Jméno	**Program budování povědomí o kybernetické bezpečnosti ve škole**
Schválení a dohled	Ředitel
Recenze	Pracovník pro informační bezpečnost školy
Frekvence kontrol	Jednou ročně nebo po jakékoli významné změně v procesu
Místo uložení	Intranet / vyhrazená složka na síťovém disku

Historie verzí

Verze	Data	Autor	Popis změn
0,1	01.10.2024	Univerzita v Coventry	Příprava návrhu šablony

Obsah

Cíl dokumentu

Cílem této politiky je zajistit, aby všichni zaměstnanci školy a studenti dostávali odpovídající školení a pravidelné aktualizace zásad a organizačních postupů týkajících se bezpečnosti informací. Vedení školy se snaží zajistit bezpečnost studentům a zaměstnancům prostřednictvím školení a dalších aktivit zvyšujících povědomí v oblasti kybernetických hrozeb.

Program budování povědomí

Program budování povědomí se zabývá následujícími tématy:

- Zásady bezpečnosti informací
- Odpovědnost za jednání studentů a zaměstnanců školy a disciplinární sankce
- Informace o hlášení incidentů
- Vzdělávání v oblasti široce pojaté digitální bezpečnosti
-

Příloha 04.1 Plán komunikace a školení v oblasti kybernetické bezpečnosti je nedílnou součástí programu. Tato příloha se aktualizuje každý rok před začátkem školního roku.

Role a odpovědnost

Školní úředník pro informační bezpečnost je pověřen vedením školy a je odpovědný za celkové fungování programu. Pedagogický personál podporuje realizaci programu. Studenti jsou povinni účastnit se programu v rámci výuky ve škole.

4.1 Plán komunikace a školení v oblasti kybernetické bezpečnosti

Vlastnosti dokumentu

Jméno	**Plán komunikace a školení v oblasti kybernetické bezpečnosti**
Název školy	Škola

Historie verzí

Verze	Data	Autor	Popis změn
0,1	01.10.2024	Univerzita v Coventry	Příprava návrhu šablony

[Škola]: Plán komunikace a školení v oblasti kybernetické bezpečnosti

Co komunikujeme?	Kdy komunikujeme?	Jak komunikujeme? (tréninková metoda)	Kdo je zodpovědný/trénuje?	pro koho?	Bylo provedeno podle plánu?	Doklady o plánované realizaci
Školní zásady bezpečnosti informací a zásady bezpečnosti informací	září	Pedagogická rada	Pracovník vedení školy/informační bezpečnosti	Učitelé a administrativní pracovníci	NE	
Zásady bezpečnosti informací	září	Edukační hodina - prezentace pravidel formou přednášky	Pracovník/pedagožka školní informační bezpečnosti	Studenti	NE	
Lekce: Phishing	říjen	Vzdělávací hodina - školení prezentace a workshop	Pracovník/pedagožka školní informační bezpečnosti	Studenti	NE	
Lekce: Hesla – jak vytvářet a spravovat hesla?	Listopad	Vzdělávací hodina - školení prezentace a workshop	Pracovník/pedagožka školní informační bezpečnosti	Studenti	NE	
Incidenty – jak reagovat na hrozby?	prosinec	Vzdělávací hodina - školení prezentace a workshop	Pracovník/pedagožka školní informační bezpečnosti	Studenti	NE	
Kyberšikana – jak jí předcházet a jak na ni reagovat?	leden	Vzdělávací hodina - školení prezentace a workshop	Pracovník/pedagožka školní informační bezpečnosti	Studenti	NE	
Dezinformace – jak rozpoznat nepravdivé informace?	únor/březen (svátky)	Vzdělávací hodina - školení prezentace a workshop	Pracovník/pedagožka školní informační bezpečnosti	Studenti	NE	
Návštěva zástupce městské stráže nebo policie	Celý rok, např. duben	Školení pro celou školu	Pozvaný zástupce	Studenti a učitelé	NE	
Ad hoc – novinky týkající se aktuálních kybernetických hrozeb	Celý školní rok	Zpravodaj a během setkání a rodičovských hodin	Pracovník/pedagožka školní informační bezpečnosti	Všichni (žáci, učitelé, rodiče)	NE	
Zprávy o účasti školy na konferencích/akcích o digitální bezpečnosti	po akci, např	Setkání, prezentace zprávy	Pracovník pro informační bezpečnost školy	Vedení, učitelé, rodiče	NE	
Prezentace studentů účastnících se projektů/soutěží digitální bezpečnosti	po akci, např	Setkání, speciální akce věnovaná kybernetické bezpečnosti	Studenti s opatrovníkem	Studenti a učitelé	NE	
Hostující přednáška zástupce rodičů pracujících v oboru kybernetické bezpečnosti	např. jednou za semestr	Přednáška	Pozvaný rodič	Studenti a učitelé	NE	
					NE	
					NE	
					NE	
					NE	
					NE	
					NE	
					NE	
					NE	
					NE	
					NE	

O autorovi

Mateusz Pękala - specialista na zvyšování povědomí o informační bezpečnosti, bezpečnostní shodě, auditu informační bezpečnosti a řízení rizik. Má dlouholeté zkušenosti jako auditor, školitel a konzultant v oblasti informační bezpečnosti. Je členem profesních organizací jako ISSA Polska a ISACA. Je certifikován v oblasti Risk and Information Systems Control™ (CRISC), Certified Information Security Professional (CISSP), Certified Data Privacy Solutions Engineer™ (CDPSE®) a Certified Information Systems Auditor® (CISA), stejně jako certifikace auditora v oblasti ISO 27001.

Více informací o projektu

CYBERSEC

EDUCHECK

https://www.coventry.ac.uk/wroclaw/

https://kreatywnidlabiznesu.pl/cyber-sec-edu-check/

https://eccedu.net/

Financováno Evropskou unií. Vyjádřené názory a názory jsou však výhradně názory autora (autorů) a nemusí nutně odrážet názory Evropské unie nebo Evropské výkonné agentury pro vzdělávání a kulturu (EACEA). Evropská unie ani EACEA za ně nemohou nést odpovědnost.

PROJEKT Č. 2023-2-PL01-KA210-VET-000176822

Spolufinancováno Evropskou unií

VŮDCE:

Research Institute Europe | Coventry University

PARTNEŘI:

STOWARZYSZENIE KREATYWNI DLA BIZNESU

EUROPEAN CENTRE FOR CAREER EDUCATION