# Vzor bezpečnostní směrnice ICT pro školy

## Úvod

V digitální době, kdy školy využívají moderní technologie pro výuku, komunikaci i správu dat, roste potřeba chránit citlivé informace, zařízení i samotný chod školy před různými riziky. Školy pracují nejen s běžnými provozními údaji, ale i s osobními a citlivými informacemi o žácích, rodičích či zaměstnancích. Jakákoli ztráta dat, kybernetický útok nebo neodborná manipulace s technologiemi může mít vážné důsledky.

Právě proto by každá škola měla mít vypracovanou vlastní bezpečnostní směrnici ICT. Ta pomáhá stanovit jasná pravidla pro práci s technologiemi, chrání data a definuje odpovědnosti jednotlivých pracovníků. Díky bezpečnostní směrnici ICT se předchází chybám, zajišťuje se soulad s legislativními požadavky a minimalizují se rizika, která s používáním moderních technologií ve školním prostředí souvisejí.

***Národní pedagogický institut vám přináší vzor takové směrnice, kterým se můžete inspirovat. Projděte si tento vzor a upravte jej dle konkrétních potřeb své školy.***

*Bezpečnostní směrnice ICT:*

* *stanoví pravidla pro řízení aktiv a rizik;*
* *člení data a informace dle jejich citlivosti a přístupu k nim;*
* *řeší přístupy jednotlivých uživatelů a jak se s nimi nakládá při změně zařazení nebo ukončení pracovního poměru;*
* *stanoví povinnosti uživatele ve škole;*
* *stanoví požadavky na zabezpečení a používání školních zařízení, přenosných školních zařízení i soukromých zařízení, přes které se přistupuje ke školním systémům;*
* *řeší způsob ukládání a zálohování dat;*
* *stanoví způsob elektronické komunikace s rodiči i žáky;*
* *řeší postup v případě kybernetického bezpečnostního incidentu.*

# Bezpečnostní směrnice ICT pro školy

**Název školy:**

**Vypracoval/a:   
Schválil/a:    
Směrnice nabývá účinnosti dne:**

## Pravidla řízení aktiv a rizik

### [Ředitel / pověřený zaměstnanec / koordinátor ICT / správce ICT] je odpovědný za:

* Identifikaci, hodnocení a evidenci aktiv.
* [Řízení rizik](https://digitalizace.rvp.cz/clanky/rizeni-kybernetickych-rizik-ve-skole), kterým jsou identifikovaná aktiva vystavena.
* **Aktivum** je informace nebo služba zpracovávaná či poskytovaná informačním a komunikačním systémem organizace.

### Pravidla použití aktiv:

* Veškerá aktiva lze použít výhradně k účelům souvisejícím s výkonem pracovní činnosti pro organizaci.
* Aktiva musí být používána v souladu s vnitřními předpisy.
* Jakékoli jiné použití aktiv musí být schváleno [*správcem ICT, ICT koordinátorem, …*].

### Pravidla pro manipulaci s dokumenty a daty

#### Veřejná informace

* Je informace primárně určená ke zveřejnění.
* Lze ji běžně sdělovat a publikovat.
* Je určena ke zpřístupnění veřejnosti, médiím apod.

#### Neveřejná informace (interní)

* Je určena pouze pro interní potřebu organizace.
* Externí přístup je povolen pouze na základě právní úpravy, smlouvy nebo se souhlasem ředitele.
* Interní přístup je omezený, uděluje se na základě oprávnění.
* Následky neoprávněného zveřejnění takové informace nejsou závažné.

#### Důvěrná informace

* Obsahuje osobní údaje nebo informace nepřístupné veřejnosti.
* Externí přístup je možný pouze dle zákona, smlouvy nebo souhlasu ředitele.
* Interní přístup je omezený.
* Následky neoprávněného zveřejnění takové informace jsou závažné.
* Důležitá je integrita a důvěrnost.

#### Chráněná informace

* Je zvláštní kategorie osobních údajů dle GDPR.
* Patří sem citlivé údaje (např. informace z PPP, hodnocení žáků, zdravotní dokumentace apod.).
* Přístup k těmto informacím má jen vybraná skupina zaměstnanců.
* Informace jsou šifrovány.
* Důvěrnost je velmi důležitá.

## Pravidla řízení přístupu

* Každý uživatel používá jedinečné přístupové jméno a heslo.
* Platí zásada „need to know“ – úroveň oprávnění odpovídá pracovnímu zařazení.
* Sdílené uživatelské účty jsou zakázány.
* Zaměstnanci mají úroveň oprávnění „standardní uživatel“.
* Jednou ročně probíhá pravidelné přezkoumávání oprávnění, zodpovědnost za přezkum má [doplňte].

### Garanti aplikací:

* Jsou odpovědní za řízení oprávnění ve své oblasti (např. účetní, personalista/ka).
* Schvalují nebo nastavují oprávnění (nebo tím pověřují ICT správce).

### 2.1. Změny oprávnění:

* Žádá o ně přímý nadřízený zaměstnance.
* Provádí je ICT správce (sítě) nebo garant aplikace.

### 2.2. Ukončení pracovního poměru:

* Přístupová oprávnění jsou po ukončení pracovního poměru zaměstnanci odebrána ke dni ukončení pracovního poměru.

### 2.3. Privilegovaná oprávnění

* Jedná se o vyšší oprávnění, než jaké má standardní uživatel.
* Mají je jen oprávněné osoby.

### 2.4. Podmínky použití privilegovaného oprávnění:

* Musí být prokazatelně potřebné.
* Držitel privilegovaného oprávnění byl prokazatelně seznámen s pravidly a odpovědností, včetně pravidel nakládání s hesly.
* Účty s privilegovaným oprávněním jsou oddělené (např. admin\_jmeno).
* Běžná práce probíhá pouze přes standardní účet, nikoliv přes admin účet.

## Bezpečnostní školení nových zaměstnanců

### 3.1. Seznámení s bezpečnostními pravidly:

* První školení probíhá při nástupu nebo před převzetím účtu a obsahuje témata jako: přihlašování, hesla, šifrování, e-mail, antivir, zálohování.
* Zaškolení k dílčím aplikacím zajišťuje garant aplikace.
* Všichni zaměstnanci projdou minimálně jednou ročně školením na témata: hesla, ochrana zařízení, sdílení dat, phishing, incidenty, umělá inteligence atd.

### 3.2. Speciální školení:

* Zaměstnanci s bezpečnostními rolemi se pravidelně účastní speciálních školení v oblasti kybernetické bezpečnosti.

## Pravidla pro řešení porušení bezpečnostní politiky

### 4.1. V případě závažného přestupku:

* Může ředitel nařídit disciplinární řízení.

### 4.2. Disciplinární komise:

* Disciplinární komise má [x] členy/ů, z toho [x] vedoucí pracovník a [x] členové z řad zaměstnanců.

### 4.3. Průběh řízení:

* Disciplinární komise posoudí míru zavinění a navrhne řediteli způsob postihu.
* Zaměstnanec má vždy možnost se k závěru komise vyjádřit.

## Pravidla při ukončení pracovního vztahu nebo změně pozice

### 5.1. Změna pracovního zařazení:

* Zaměstnanec vrátí stávající zařízení oproti protokolu o předání.
* Následně jsou mu odebrána jeho oprávnění a přidělena oprávnění nová.

### 5.2. Ukončení pracovního vztahu:

* Zaměstnanec vrátí svěřená zařízení oproti protokolu o předání.
* Následně jsou mu zrušena všechna oprávnění.
* Zaměstnanci nejsou před ukončením pracovního poměru oprávněni kopírovat informace, ke kterým nemají oprávnění.

## Školní účty

* Všichni uživatelé mají zřízený účet do školního informačního systému [*např. Bakaláři, Edookit, EduPage, ŠkolaOnline aj*.].
* Všichni uživatelé mají zřízený účet do cloudových služeb [*Microsoft 365 nebo Google*] s e-mailovou adresu ve formátu [jan1234@doménaškoly.cz – užívat e-mail [jméno.příjmení@škola.cz](mailto:jméno.příjmení@škola.cz) není doporučeno, neboť se jedná o osobní údaj].
* V případě ztráty hesla se uživatel obrátí na [helpdesk].
* Povinnosti uživatele školního účtu jsou popsány v části 7. Pravidla bezpečného chování uživatele.

## Pravidla bezpečného chování uživatele

* Organizace může monitorovat užívání ICT prostřednictvím monitoringu a kontrol.
* K práci na školních digitálních zařízeních (počítačích, tabletech) je oprávněn pouze pověřený zaměstnanec s unikátními přístupovými údaji (uživatelské jméno a heslo).
* K práci na školních digitálních učebních pomůckách (počítačích, tabletech) je oprávněn pouze žák s unikátními přístupovými údaji (uživatelské jméno a heslo).

### 7.1. Povinnosti uživatele:

* Uživatel je povinen používat přidělené přihlašovací údaje.
* Změnit heslo při prvním přihlášení, je-li k tomu vyzván.
* Uchovávat heslo v tajnosti.
* Zabránit odpozorování hesla.
* Nepoužívat „zapamatovat heslo“ v prohlížeči.
* Pravidla pro tvorbu hesla:
* Heslo obsahuje min.\_\_\_ znaků.
* Heslo obsahuje malá a velká písmena, číslice a speciální znak.
* Heslo nesmí obsahovat jméno uživatelského účtu nebo části jména a příjmení uživatele.
* Heslo neobsahuje známá jména, osobní údaje a jiná lehce odhalitelná hesla (např. datum narození, jména členů rodiny, názvy předmětů v blízkosti počítače, běžných jednoduchých slov umožňujících tzv. slovníkový útok apod.).
* Další pravidla:
* Platnost hesla je: max. \_\_ měsíců, min. \_\_ hodin.
* Historie: \_\_ hesel.
* Je povoleno max. \_\_ neúspěšných pokusů, poté je účet zablokován.
* Blokace účtu: \_\_\_ minut.
* V případě podezření na kompromitaci hesla je nutné okamžitě heslo změnit a vše nahlásit.
* Při opuštění pracoviště má uživatel zařízení uzamknout.
* Pravidlo „prázdného stolu“:
* Žádné citlivé dokumenty by neměly zůstávat volně položené na stole nebo v tiskárně.
* Notebooky a přenosná zařízení by měla být uložena v uzamčených skříňkách nebo zabezpečena (např. zámkem).
* Přístupové karty, USB disky, klíče ukládá uživatel na bezpečné místo, nenechává je na stole.
* Jestliže uživatel opustí pracoviště, byť jen na chvíli, uzamkne počítač (např. klávesovou zkratkou Win + L).
* Dokumenty obsahující citlivé údaje by měly být skartovány, ne vyhazovány do běžného koše.
* Uživatel dodržuje pravidlo „prázdné obrazovky“, tj. dokumenty otevřené na obrazovce zařízení nejsou přístupné neoprávněným osobám.
* Uživatel neinstaluje na zařízení žádný software.
* Nestahuje žádné soubory z neautorizovaných stránek.
* Nezasahuje do zařízení a jeho konfigurace, vyjma situací, kdy ho o to požádá správce ICT / koordinátor ICT.
* Uživatel řádně zálohuje svá pracovní data dle postupů stanovených správcem ICT.
* Nekopíruje, neukládá, nepřenáší žádná data organizace mimo její prostory.
* Nepoužívá pro výkon pracovní činnosti soukromé či neznámé datové nosiče (např. CD, flash disky, externí HDD).
* Nenavštěvuje rizikové internetové stránky a nekliká na reklamní bannery na webových stránkách.
* Ověřuje doručenou elektronickou poštu a v případě podezření, že se jedná o závadný e-mail (spam, podvodný e-mail apod.), takovou zprávu neotvírá, nereaguje na ni a tuto skutečnost neprodleně ohlásí [*správci ICT nebo vedoucímu zaměstnanci*].
* Uživatel netiskne data ani citlivé údaje pro jiné než pracovní účely.
* Zasílá-li uživatel e-mail s šifrovanou přílohou, předává příjemci heslo jinou cestou  (např. telefonicky, formou SMS apod.). Heslo nikdy nesmí být součástí odesílaného e-mailu. Hesla k jednotlivým souborům se řídí stejnými pravidly jako hesla k uživatelským účtům.
* **Uživatel neprodleně ohlásí kompromitaci nebo ztrátu jakéhokoliv zařízení či dat** [*správci ICT / koordinátoru ICT / vedoucímu zaměstnanci*].
* Veškeré požadavky na nákup [softwaru, programového vybavení, spotřebního materiálu] konzultují zaměstnanci s [*ICT koordinátorem / zástupcem ředitele / IT správcem…]*. [*ICT koordinátor* */ zástupce ředitele / IT správce*] předává požadavky k posouzení vedení školy.

## Pravidla pro ochranu a používání přenosných zařízení

### 8.1. Ochrana přenosných zařízení:

* Zaměstnanci mají povoleno vykonávat pracovní činnost mimo objekty organizace pouze po schválení vedoucím zaměstnancem.
* Za ochranu přiděleného přenosného zařízení je vždy odpovědný zaměstnanec.

### 8.2. Ochrana soukromých zařízení:

* Zaměstnanec bere na vědomí, že převzetím přístupových oprávnění k místním aplikacím přebírá odpovědnost za zajištění minimální úrovně ochrany soukromých zařízení, kterou je povinen při přístupu k místním aplikacím zajistit.
* Pořizují-li zaměstnanci audiovizuální materiál obsahující fotografie či nahrávky žáků, činí tak v souladu s platnou legislativou a výhradně na zařízení organizace. Pořídí-li zaměstnanec záznam na soukromé zařízení, přebírá osobní odpovědnost za bezpečné nakládání s těmito údaji dle § 84–90 občanského zákoníku.
* Je-li nezbytné použít k záznamu soukromé zařízení, musí zaměstnanec neprodleně (nejpozději do 48 hodin) přenést fotografie do školního úložiště, odstranit je ze svého zařízení i ze soukromých cloudových služeb a provést o tom záznam.
* Dojde-li ke ztrátě či jinému zneužití soukromého zařízení, které by mohlo obsahovat záznamy žáků, zaměstnanec informuje [*správce ICT*].
* Soukromá zařízení, jejichž prostřednictvím zaměstnanec přistupuje k místním aplikacím, musí být:

1. Vybavena pravidelně aktualizovaným operačním systémem.
2. Vybavena pravidelně aktualizovanou antivirovou aplikací.
3. Chráněna pomocí přihlašovacích údajů uživatele, a to za těchto podmínek:

* Minimální délka hesla je 8 znaků.
* V hesle musí být použité alespoň 3 ze 4 skupin znaků (malá písmena, velká písmena, číslice nebo speciální znaky).
* Soukromé zařízení musí být nastaveno tak, aby se po 5 minutách neaktivity uživatele uzamklo, v případě smartphonu a tabletu po 2 minutách neaktivity.

1. Smartphony a tablety musí být chráněny PINem, biometrickým údajem nebo heslem s alespoň 6 znaky.
2. Soukromá zařízení musí být vybavena pouze aplikacemi instalovanými z oficiálních obchodů (např. Google Play, Apple store, Microsoft store, Galaxy store apod.).
3. Úložiště zařízení musí být zašifrováno.

### 8.3. Pravidla pro používání přenosných a soukromých zařízení

Při používání přenosných a soukromých zařízení pro připojení k místním aplikacím jsou zaměstnanci povinni:

1. Učinit všechna dostupná opatření, která mohou zabránit ztrátě či odcizení zařízení (neponechávají je bez dohledu a nebo zabezpečení např. v dopravních prostředcích, v ubytovacích zařízeních apod.).
2. Pro připojení k internetu prostřednictvím wi-fi sítě využívají zaměstnanci pouze šifrovaného zabezpečeného připojení (připojení prostřednictvím hesla, důvěryhodný poskytovatel – úřad, pořadatel školení apod.) a po ukončení práce se od místních aplikací odpojují (nelze využívat např. free wi-fi v nákupních centrech, hotelích, nádražích apod.).
3. Aktivně zabraňovat odpozorování obrazovky cizí osobou (např. ve vlacích, restauracích, na lavičkách, v prostředcích hromadné dopravy apod.).
4. Neumožnit jiným osobám, včetně rodinných příslušníků, přístup k informacím zpracovávaným v místních aplikacích.

## Pravidla bezpečného používání zařízení organizace

Zařízení organizace, jejich prostřednictvím je možné přistupovat k místním aplikacím musí splňovat minimálně tyto podmínky:

1. Jsou vybavena pravidelně aktualizovaným operačním systémem.
2. Jsou vybavena pravidelně aktualizovanou antivirovou aplikací.
3. Jsou chráněna pomocí přihlašovacích údajů uživatele (viz část 7. Pravidla bezpečného chování uživatele).
4. Jsou nastavena tak, aby se po 10 minutách neaktivity uživatele uzamkla, v případě smartphonu a tabletu po 2 minutách neaktivity.
5. Jsou nastavena tak, aby uživatel disponoval pouze účtem s oprávněním „standardní  uživatel“.
6. Smartphony a tablety jsou chráněny PINem, biometrickým údajem nebo heslem s alespoň 6 znaky.
7. Jsou vybavena pouze schválenými aplikacemi.
8. U přenosných zařízení je pevný disk šifrován, pokud to operační systém umožňuje.
9. Vyměnitelné médium (např. USB disk, externí pevný disk apod.) je připojeno k pracovní stanici nebo přenosnému zařízení a zkontrolováno antivirovým softwarem.
10. Pokud se do vyměnitelného média ukládají data z místních aplikací, je toto médium  šifrováno.

Správce ICT / koordinátor ICT odpovídá za nastavení zařízení, která se připojují k místním aplikacím, dle výše uvedených pravidel.

\_\_\_\_\_\_\_ ve spolupráci se správcem ICT stanovuje pravidla pro centralizovanou správu zařízení, včetně přenosných zařízení.

## Ukládání a zálohování dat

### Pravidla pro ukládání a zálohování dat

* Data jsou ukládána na školní server, na disk [*doplňte*], kde má každý uživatel přístup pouze ke svému prostoru.
* Školní matrika [*doplňte*] je uložena na disku [doplňte], aplikace běží v [*cloudové službě poskytovatele softwaru*/*serveru*].
* Účetní systémy a databáze jsou uloženy na [*serveru*], uživatelé mají k dispozici klientskou část lokálně na svém zařízení.
* Všechna data jsou automaticky zálohována dle pravidla 3-2-1: (1) cloudovou službou, (2) na [NAS] a na (3) [externí disk (např. Windows Server 2019/2022)] každý den.
* Pro přenos a ukládání dat se využívá:
  1. lokální síť,
  2. VPN,
  3. [cloudové úložiště], kde má každý zaměstnanec svůj účet.

### Antivirová ochrana

* Na všech počítačích jsou nainstalovány [tři typy] antivirového programu s automatickou aktualizací přes internet [případně doplňte, jakým způsobem je antivirový program aktualizován].
* Antivirová ochrana funguje centrálně:

1. Příchozí komunikace je nejprve kontrolována na vstupním bodu školní vnitřní sítě.
2. Následně probíhá kontrola i na jednotlivých stanicích.
3. Je aktivní IDP (Intrusion Detection and Prevention) – ochrana proti průnikům a krádeži dat.

### Zabezpečení dat

* Škola používá [firewall ....] se zapnutými službami:
  1. Content filter,
  2. IDP Signature,
  3. Application Patrol.
* Firewall zajišťuje bezpečný přístup k internetu a blokuje (pozn.: blokování lze zajistit i externí službou):
  1. [nevhodné weby – např. erotika, hacking, drogy],
  2. [aplikace sociálních sítí pro žáky],
  3. [další nevhodný obsah dle pravidel školy].

## Komunikace

1. Škola zpracovává osobní údaje na základě čl. 6 odst. 1 písm. c) Obecného nařízení (GDPR), tedy pro splnění právní povinnosti. Jedná se plnění právních povinností podle zákona č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon).
2. Škola spravuje následující sociální sítě [Facebook, Instagram]. Tyto účty spravují pouze určení zaměstnanci.
3. Pro komunikaci s rodiči i žáky je určen oficiální jednotný kanál [školní informační systém, Microsoft 365, Google Education aj.].
4. Pro interní komunikaci ve škole je používán oficiální jednotný kanál [školní informační systém, interní komunikační systém].
5. Zaměstnanci nevytvářejí neoficiální komunikační kanály s žáky ani rodiči (facebookové skupiny, WhatsApp skupiny aj.).

## Kybernetické bezpečnostní incidenty

### 12.1. Povinnosti uživatele

* Jakoukoliv závadu nebo podezření na nestandardní chování počítače či jeho periferií je nutné bez odkladu nahlásit na [*helpdesk / IT správci*] nebo nadřízenému.
* Závadnou techniku není dovoleno používat.
* **V případě zjištění kybernetické bezpečnostní události jsou zaměstnanci povinni neprodleně informovat [*helpdesk, IT správce, ICT koordinátora*].**

### 12.2. Kybernetickou bezpečnostní událostí může být mimo jiné:

1. ponechání přihlášeného zařízení bez dozoru,
2. zachycení nevyžádaného e-mailu s přílohou (např. výzva k zaplacení faktury),
3. podezření na kompromitaci přihlašovacích údajů,
4. nalezení neznámého flash disku apod.

### 12.3. Kybernetickým bezpečnostním incidentem může být mimo jiné:

1. ztráta zařízení (notebooku, flash disku, smartphonu apod.),
2. zjištění použití hesla jinou osobou,
3. napadení škodlivým softwarem,
4. narušení fyzické bezpečnosti organizace/kanceláře,
5. předání přihlašovacích údajů jiné osobě (včetně kolegů či vedoucích) apod.

### 12.4. Postup v případě podezření na kybernetický incident

Ředitel nebo jím pověřená osoba:

1. Posoudí kybernetickou bezpečnostní událost/incident a její dopady na organizaci, data nebo na používání místních aplikací.
2. Pokud je vyhodnoceno, že se jedná o bezpečnostní incident, musí být přijata okamžitá opatření k zastavení případného šíření incidentu (např. ředitel vydá varování zaměstnancům PO: „Neotevírejte přílohu e-mailu s předmětem …, příloha je nositelem viru!“).
3. Po zastavení šíření incidentu je nezbytné zdokumentovat rozsah a dopady incidentu pro pozdější vyhodnocení a analýzu.
4. Pro záznam informací lze použít, dle charakteru incidentu, notebooky, diktafony, digitální fotoaparáty, příp. i poznámkový blok. Všechny pořízené materiály musí být bezpečně uloženy a označeny pro evidenci důkazů ke konkrétnímu bezpečnostnímu incidentu.
5. Záznam o incidentu by měl obsahovat alespoň:
   1. Datum incidentu
   2. Vyšetřující osobu/osoby
   3. Popis incidentu:

* Kde incident vznikl (fyzické místo anebo technologie)
* Příčina vzniku incidentu
* Dopad incidentu
  1. Návrh opatření
  2. Ředitel nebo jím pověřená osoba zavede nápravná opatření, vyhodnotí jejich účinnost a následně seznámí zaměstnance s kybernetickým bezpečnostním incidentem a jeho příčinami.

**V případě vážného kybernetického incidentu (kybernetického útoku, kompromitace sítě aj.) postupujte podle** [**Krizového plánu**](https://digitalizace.rvp.cz/napric-predmety/kyberneticka-bezpecnost#predchazeni) **(viz příloha).**