

Střední škola řemeslná a Základní škola,  
Soběslav, Wilsonova 405  
IČO: 72549572



# **SMĚRNICE UPRAVUJÍCÍ PROVOZ INFORMAČNÍCH A KOMUNIKAČNÍCH TECHNOLOGIÍ**

Platnost od 25.5.2018

**S  
Š  
Ř  
a  
Z  
Š  
S  
o  
b  
ě  
s  
l  
a  
v**

### Použité zkratky a zástupná označení

Zkratka	Popis
<b>DPIA</b>	Posouzení vlivu na ochranu osobních údajů (Data Protection Impact Assessment)
<b>IP adresa</b>	Jednoznačná identifikace zařízení v počítačové síti
<b>Pověřenec</b>	Pověřenec pro ochranu osobních údajů
<b>Legislativní rámec</b>	Zákon 101/2000 Sb. o ochraně osobních údajů, ve znění pozdějších předpisů, Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, Zákon č. 89/2012 Občanský zákoník, Zákon o ochraně osobních údajů, kterým bude zrušen, resp. nahrazen Zákon 101/2000 Sb. (dle návrhu 55/2018 Sb.)
<b>MAC</b>	Jednoznačný identifikátor síťového zařízení (tzv. fyzická adresa)
<b>Obecné nařízení</b>	Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
<b>Garant agendy</b>	Osoba odpovědná za agendu zpracování osobních údajů
<b>ICT pracovníci</b>	ICT technik; metodik a koordinátor ICT
<b>OÚ</b>	Osobní údaje
<b>Organizace</b>	Střední škola řemeslná a Základní škola, Soběslav, Wilsonova 405
<b>ZOÚ</b>	Zaměstnanec odpovědný za ochranu osobních údajů v Organizaci

## ČÁST I - ÚVODNÍ USTANOVENÍ

### Článek 1

#### PŘEDMĚT ÚPRAVY

- 1) Tato směrnice stanovuje pravidla provozu informačních a komunikačních technologií, provozu počítačové sítě, chování jejich uživatelů, nakládání s hardware, software a audiovizuální technikou (dále jen „**IKT**“) na **Střední škole řemeslné a Základní škole, Soběslav, Wilsonova 405** (dále jen „**SŠŘ**“).
- 2) Příloha k této směrnici stanovuje pravidla uživatelské podpory, pohotovosti, komunikace a řešení havárií v oblasti IKT.
- 3) Tato směrnice je závazná pro všechny uživatele IKT v SŠŘ.
- 4) Uživatelem IKT je
  - a) Zaměstnanec SŠŘ a ZŠ Soběslav s platnou pracovní smlouvou, dohodou o provedení práce nebo dohodou o pracovní činnosti;
  - b) Řádný student pouze v době výuky na učebnách PC v rámci oddělené zabezpečené sítě.
  - c) Další fyzická osoba s odůvodnitelným vztahem k SŠŘ (zástupce dodavatele, účastník konference, student na výměnném pobytu apod.), již bylo povoleno na základě žádosti využití IKT.

### Článek 2

#### ZÁKLADNÍ POJMY

- 1) **Hardware** - souhrn technických prostředků výpočetní a komunikační techniky, jde především o počítače a jejich komponenty, periferie (tiskárny, monitory apod.) včetně všech jejich komponentů a prvků datových sítí včetně jejich komponent.
- 2) **Software** - programové vybavení hardwarových prostředků.
- 3) **Login** - unikátní uživatelské jméno, řetězec písmen a číslic, který spolu s heslem umožňuje přístup do elektronických aplikací.
- 4) **Heslo** - neveřejný řetězec písmen, číslic a znaků pro přístup k elektronickým systémům SŠŘ.
- 5) **Certifikát** - elektronický dokument, kterým se prokazuje totožnost jeho držitele.
- 6) **Licence** - oprávnění k výkonu práva užívat software stanovené licenční smlouvou nebo licenčním ujednáním.
- 7) **Licenční smlouva a licenční ujednání** - právní dokument, kterým autor poskytuje nabyvateli oprávnění k výkonu práva užití software stanoveným způsobem a ve stanoveném rozsahu.
- 8) **Pracovní stanice** - osobní počítač včetně nezbytných periférií.
- 9) **Notebook** - přenosný osobní počítač.
- 10) **Server** - prostředek v počítačové síti, který poskytuje služby klientům.
- 11) **Klient** - zařízení v počítačové síti, využívající služeb serveru.
- 12) **DHCP (Dynamic Host Configuration Protocol)** - protokol pro automatické přidělování IP adres jednotlivým osobním počítačům v počítačových sítích.
- 13) **Wi-Fi (Wireless Fidelity)** - bezdrátové připojení k síti.
- 14) **RFC (Request for Comments)** - označení doporučených standardů.
- 15) **DoS (Denial of Service)** - typ útoku na přetížení služeb a serverů.

- 16) P2P (Peer-to-peer) - výměnné sítě, kde spolu komunikují klienti této sítě přímo.
- 17) IPv4 - Internet Protocol verze 4.
- 18) IPv6 - Internet Protocol verze 6.
- 19) Intranet - privátní počítačová síť, která je izolovaná od dalších vnějších sítí.
- 20) Doménové jméno (internetová/intranetová doména) - jednoznačné jméno (identifikátor) počítače nebo počítačové sítě, které jsou připojené do intranetu nebo internetu. Příkladem doménového jména je www.srsobeslav.cz.
- 21) IS - informační systém.

## ČÁST II - NAKLÁDÁNÍ S ICT MAJETKEM SŠŘ

### Článek 3

#### POŘÍZENÍ, REGISTRACE A EVIDENCE

- 1) Pořízení ICT majetku realizuje pouze hospodářka školy ve spolupráci s ICT technikem (správcem sítě).
- 2) Hmotný i nehmotný ICT majetek je evidován v ekonomickém informačním systému Fénix.
- 3) Každé ICT zařízení musí být řádně zařazeno do užívání a zaevidováno do operativní evidence na SŠŘ.
- 4) Předepsané revize a zkoušky počítačového hardware a audiovizuální techniky podle příslušné české technické normy zajišťuje pověřený zaměstnanec (učitel OV uč.oboru Elektrikář).

## ČÁST III - UŽIVATELÉ ICT SŠŘ

### Článek 4

#### OBECNÉ CHOVÁNÍ UŽIVATELŮ

- 1) Uživatel ICT SŠŘ se musí chovat tak, aby neporušoval platný právní řád České republiky a interní směrnice SŠŘ.
- 2) Uživatel je povinen zejména:
  - a) Hlásit bez prodlení nadřízenému pracovníkovi nebo ICT technikovi jakékoliv podezření na porušení této směrnice, závadné chování uživatelů ICT (např. zneužití přístupu do sítě, podezření na nelegální činnost, odcizení či zneužití dat), závady hardware, podezření na nelegální software, chyby v softwaru neaktuálnosti softwaru;
  - b) Využívat ICT SŠŘ pouze pro pracovní či vzdělávací účely, doplňkovou činnost nebo úkoly související s provozem a správou SŠŘ;
  - c) Užívat k práci na pracovní stanici nebo notebooku ve vlastnictví SŠŘ pouze legální software, který je určený pro jeho práci nebo studium a instalovaný ICT pracovníky (ICT technik nebo metodik a koordinátor ICT) nebo s jejich vědomím;
  - d) Pravidelně čist (alespoň 1x za pracovní den) a v přiměřeném čase odpovídat na elektronickou poštu v e-mailové schránce SŠŘ, byla-li mu zřízena.
- 3) Uživatel nesmí zejména:
  - a) Využívat ICT SŠŘ k soukromým, komerčním nebo jiným účelům nesouvisejícím s činnostmi SŠŘ;

- b) Vystavovat prostředky ICT jakémukoliv nebezpečí;
- c) Zprostředkovat přístup k ICT SŠŘ fyzickým či právnickým osobám, které nejsou uživateli ICT SŠŘ;
- d) Jakýmkoli způsobem poškozovat jakoukoli součást ICT SŠŘ;
- e) Používat prostředky ICT v počítačové síti SŠŘ, která nejsou v majetku SŠŘ;
- f) Odstraňovat informace nebo označení identifikující autorská práva k software;
- g) Pracovat pod cizí identitou, používat prostředky k jejímu získání nebo zneužití v tomto pochybení či nedbalosti jiného uživatele, vyjma ICT pracovníků za účelem testování a nastavení na základě udělené výjimky vedením organizace;
- h) Sledovat nebo odposlouchávat provoz sítě;
- i) Spouštět nebo instalovat software neúměrně zvyšující zatížení sítě a vyvarovat se další činnosti, která vede k zatížení sítě nebo omezení služeb. Jedná se především o používání výměnných sítí (P2P, DDoS útoky nebo další softwarové nástroje);
- j) Zapojovat do sítě zařízení, která mohou ovlivnit komunikační provoz sítě (např. přepínače, směrovače aj.).
- k) Na svých zařízeních v síti SŠŘ používat serverové aplikace nebo skenovací a penetrační nástroje. Jedná se zejména o síťové doménové řadiče, dhcp servery, licenční servery apod.;
- l) Provádět výměny, stěhování, čištění, odpojení či připojení k datové síti, opravy a změny konfigurace software, hardware a jeho částí (klávesnice, tiskárny, monitory apod.) bez účasti zaměstnance - ICT technika. Výjimku tvoří odpojení a připojení přenosných datových nosičů. Stěhování v rámci organizace, jehož součástí je stěhování hardware, musí být předem konzultováno s ICT technikem nebo s metodikem a koordinátorem ICT a musí být definovány případné náklady a změny (potřeba změn v konfiguraci počítačové sítě aj.).

## **Článek 5**

### **PRÁCE S PŘÍSTUPOVÝMI INFORMACEMI**

- 1) Účet zaměstnance je zřízen na základě zadání uživatele do systému, a to do druhého dne od zadání požadavku.
- 2) Uživatel je oprávněn používat pouze přidělený login. Login je vždy unikátní, daný ICT technikem a neměnný. Přidělené heslo je uživatel povinen si změnit po prvním přihlášení do IS a dále ho obměňovat každé 3 měsíce. Uživatel je povinen udržovat heslo v tajnosti a neumísťovat písemnou formu na místo, které je dostupné dalším osobám.
- 3) Pomocí přiděleného loginu a hesla se přistupuje do elektronických aplikací SŠŘ.
- 4) Přístup do dalších systémů vytváří ICT technik. Každý uživatel si může změnit heslo. Při změně hesla se nedoporučuje používat například: jména osob, data narození, rodná čísla, registrační značky motorových vozidel, jméno počítače nebo telefonní čísla.
- 5) Účet zaměstnance je zrušen po zadání informace o ukončení pracovněprávního vztahu k SŠŘ ICT technikovi.

## **Článek 6**

### **STUDENTI**

- 1) Student užívá hardware a software školy pro účel, ke kterému je určen. Jde zejména o využívání počítačů, zařízení a aplikací pro studium a samostudium.
- 2) Před opuštěním pracovní stanice je student povinen se odhlásit ze všech aplikací a operačního systému.

- 3) Student není oprávněn se připojovat s vlastním zařízením do sítě SŠŘ jinak než přes Wi-Fi, nebo na místech k tomu určených.
- 4) Student je povinen pro přidělení IP adresy u vlastního zařízení použít protokolu DHCP. Nastavení statické adresy je zakázáno.
- 5) Odpovědnost za své zařízení nese student. Odpovídá především za zabezpečení zařízení (notebooky, notepad, telefony aj.), antivirovou ochranu a software. V případě zjištění problému s výše uvedenými body, je správce sítě oprávněn zařízení odpojit a vlastníka informovat. Po odstranění zaslát informační problému je možné přístup opět povolit.
- 6) Škola může poskytnout studentům software, který ze svého licenčního ujednání lze použít pro studenty a samostudium.

## Článek 7

### ZAMĚSTNANCI

- 1) Základní zásady ochrany dat na pracovních stanicích a notebookech (počítačích), které jsou ve vlastnictví SŠŘ, jsou následující:
  - a) Zaměstnanec je oprávněn využívat k práci pouze počítač, který byl k jeho práci určen (byl mu přidělen) nebo počítače v místnostech určených pro výuku.
  - b) Přístup zaměstnanců na počítač přidělený jinému zaměstnanci je možný pouze se svolením jeho uživatele, a to vždy pouze pod vlastní identitou. Zaměstnanec smí umožnit přístup na přidělený počítač pouze uživatelům ICT SŠŘ.
  - c) Při opuštění pracoviště učiní zaměstnanec nezbytná opatření k zabránění zneužití přístupu k datům některou z možností danou operačním systémem (například formou řádného odhlášení se z aplikace a uzamčením pracovní stanice nebo jejím vypnutím) a dále zabezpečí pracoviště před vstupem neoprávněné osoby.
  - d) Šifrování dat a disků, pokud není řešeno ve spolupráci s ICT technikem, není povoleno.
- 1) Pracovní stanice a notebooky zaměstnanců jsou všechny připojeny do internetu prostřednictvím počítačové sítě SŠŘ. Výjimkou může být odůvodněné rozhodnutí nadřízeného pracovníka nebo odpojení pracovní stanice nebo notebooku z důvodu bezpečnosti.
- 2) Zakazuje se otevírat nebo odesílat přílohy se soubory umožňující spustit škodlivý kód. Jedná se zejména o soubory s příponou - exe, bat, com, dll, lnk, msi, reg, 386, bin, chm, cmd, vbs a podobné
- 3) Pokud práce se softwarovou aplikací vyžaduje přihlášení, smí být zaměstnanec přihlášen jen po nezbytně nutnou dobu, tzn. po dobu, po kterou s aplikací software skutečně pracuje.

## Článek 8

### ICT PRACOVNÍCI

- 1) ICT pracovníci jsou oprávněni k přístupu ke všem pracovním stanicím a notebookům ve vlastnictví SŠŘ a k datům na nich uloženým. Musí přitom dbát, aby jejich počínání bylo v souladu se zákonem na ochranu osobních údajů.
- 2) ICT pracovníci mají rozděleny kompetence, přístupy a správu ICT takto:

- ICT technik - kompletní správu ICT v rámci celé sítě SŠŘ
- Metodik a koordinátor ICT - správu ICT v učebnách PC.

Provoz sítě, aplikací a přístupu k nim může být monitorován. Priority řešení problémů určuje ICT technik po konzultaci s vedením SŠŘ.

- 3) ICT pracovníci mají povinnosti zejména:
- a) Chránit zabezpečení ICT SŠŘ.
  - b) Chránit uživatelské a administrátorské přístupové údaje na servery, datová úložiště a do aplikací.
  - c) Poskytovat uživatelskou podporu, konzultace a pomoc uživatelům.
  - d) Zajišťovat pravidelné školení bezpečnosti ICT nových a stávajících zaměstnanců;
  - e) Nesdělovat přístupové informace na zařízení a aplikace organizace třetím osobám, dodavatelům i dalším zaměstnancům, kteří nemají provoz daného serveru nebo aplikace v kompetenci.
  - f) Starat se o údržbu a kontrolu software a hardware pracovních stanic, notebooků a jejich antivirovou ochranu. Správci sítě mají plný přístup k určeným zařízením a musí jim být umožněn přístup k software a hardware.
  - g) Starat se o zajištění infrastruktury a telekomunikací školy. Kontrolují funkčnost sítě, připojení do internetu a sledují provoz sítě. K tomuto účelu mohou používat patřičné nástroje.
  - h) Zajišťovat instalace učeben, kanceláří a pracovních stanic. Zajišťovat a kontrolovat přístupy do sítě SŠŘ.
  - i) Zajišťovat chod kopírovacích zařízení.
  - j) Plnit další povinnosti vyplývající z interních směrnic SŠŘ.

## ČÁST IV - PROVOZ NA SERVERECH A NAKLÁDÁNÍ S DATY

### Článek 9

#### PROVOZ NA SERVERECH

- 1) Poštovní servery:
- a) Zaměstnanci (podle pracovního zařazení) mají přidělen pracovní poštovní účet (e-mail).
  - b) Přesměrování e-mailů mimo doménu srsobeslav.cz není povoleno. ICT technik je povinen zveřejnit návod a poskytnout součinnost při nastavení e-mailových klientů uživatelů tak, aby uživatel mohl své e-maily číst v jednom e-mailovém klientovi.
  - c) Velikost přílohy e-mailu je omezena na 20 MB.
  - d) Pošta ve složce Nevyžádaná pošta starší 7 dnů je automaticky smazána.
  - e) Pošta ve složce Koš starší 30 dnů je automaticky smazána.
- 2) Souborové servery:
- a) Každý zaměstnanec SŠŘ má přiděleno diskové úložiště tzv. home.
  - b) Přístup do dalších umístění souborového serveru je dán pracovním zařazením.
  - c) Za obsah diskového úložiště (home) ručí vždy majitel účtu, za obsah na sdíleném diskovém úložišti ručí jeho vlastník. Obsah může být automaticky promazáván o nebezpečné typy souborů a soubory audio a video. Uživatel je o smazání obsahu informován. V případě žádosti o obnovu dat, je možné okamžitě obnovit data do stáří 14 dnů nebo obnovit soubory ze starších záloh, pokud jsou k dispozici.

## Článek 10

### PRÁCE A NAKLÁDÁNÍ S DATY

- 1) Uživatelé jsou povinni při nakládání s daty, tzn. při jejich pořizování, zpracovávání, archivaci a šíření, dodržovat obecně závazné právní předpisy České republiky a interní směrnice SŠŘ.
- 2) Uživatel je povinen zajistit ochranu dat před zneužitím a ztrátou. SŠŘ neodpovídá za ztrátu a zneužití dat způsobené nedbalostí či chybou uživatele.
- 3) Pořizování a nakládání s databázemi, datovými sadami či jinými celistvými datovými strukturami, které nejsou volně šiřitelné, musí být vždy podloženo smluvním ujednáním s poskytovatelem těchto dat. Smluvní ujednání musí obsahovat zejména podmínky a způsob, jak je SŠŘ oprávněna s daty nakládat, včetně možnosti a rozsahu jejich dalšího šíření. Nestanoví-li obecně závazné právní předpisy jinak, musí být tyto podmínky sjednány v písemné smlouvě.
- 4) Není-li si uživatel jist jakýmkoliv aspektem pořizování, zpracovávání, archivaci a šíření dat, zpracováním osobních údajů je povinen konzultovat problematiku s nadřízeným pracovníkem a ten v případě potřeby následně s ZOÚ nebo pověřencem pro ochranu OÚ.

## ČÁST V - ZÁVĚREČNÁ USTANOVENÍ

### Článek 11

#### PORUŠENÍ PRAVIDEL A SANKCE

- 1) Při porušení pravidel stanovených touto směrnicí, případně dalšími obecně závaznými právními předpisy v oblasti ICT (dále jen „pravidla“), se postupuje vždy vzhledem k závažnosti tohoto porušení.
- 2) Při jakémkoliv zjištění porušení pravidel se nejprve zajistí náprava tak, aby nedošlo ke škodě na majetku, zdraví či nedošlo k přestupku nebo trestnému činu. Pokud již došlo ke škodě či přestupku nebo trestnému činu je povinností všech zúčastněných stran co nejvíce minimalizovat škody či dopad na provoz SŠŘ.
- 3) Povinností uživatele ICT je hlásit ICT technikovi jakékoliv porušení či podezření na porušení pravidel (čl. 4, odst. 2, písm. a této směrnice). Povinností ICT technika je problémovou situaci neprodleně řešit (vč. navržení sankcí za porušení pravidel a návrhu dalšího postupu) s
  - a) bezprostředně nadřízeným zaměstnancem, týká-li se porušení či podezření na porušení pravidel uživatele uvedeného v čl. 1, odst. 4, písm. a),
  - b) věcně příslušným vedoucím zaměstnancem, týká-li se porušení či podezření na porušení pravidel uživatele uvedeného v čl. 1, odst. 4, písm. b),



## Článek 12

### ZÁVĚREČNÁ USTANOVENÍ

- 1) Směrnicí se ruší Směrnice k ochraně dat zpracovaných výpočetní technikou a ochrana osobních údajů ze dne 1.3.2012.
- 2) Směrnice nabývá platnosti dne 25.5.2018.
- 3) Směrnice bude zveřejněna v informačním systému zaměstnancům - Intranet. a na [www.ssrsobeslav.cz](http://www.ssrsobeslav.cz)

V Soběslavi, dne 23.5.2018

**Střední škola řemeslná a Základní škola,  
Soběslav, Wilsonova 405  
IČ: 72549572**

⑦



.....  
Darja Bártová, ředitelka školy

**Přílohy:** Příloha 1 - Uživatelská podpora, pohotovost, řešení havárií a komunikace v ICT SŠŘ

## **Příloha 1 - Uživatelská podpora, pohotovost, řešení havárií a komunikace v ICT SŠŘ**

### **UŽIVATELSKÁ PODPORA ICT**

Uživatelskou podporu v oblasti ICT provádí ICT pracovníci:

- ICT technik - tel. 724 136 683, email: spaleservis@cbox.cz
- Metodik a koordinátor ICT - tel. 389 822 811, fiala.radek@srsobeslav.cz

#### **Pro zaměstnance zajišťuje podporu ICT technik:**

- 1) Běžné řešení problémů (přes Helpdesk, telefon, e-mail, osobně):
  - a) Žádosti o individuální školení;
  - b) Žádosti o přípravu AV a IT techniky;
  - c) Problém s počítačem v kanceláři nebo služebním notebookem;
  - d) Žádost o změnu, výměnu telefonu;
  - e) Základní uživatelská podpora pro elektronické systémy (IS, E-Learning, Web);
  - f) Akutní problémy s přihlášením obecně;
  - g) Další dle aktuálních potřeb.

**Pro studenty zajišťuje podporu učitel ICT (metodik a koordinátor ICT) v době výuky.**

### **HAVÁRIE ICT**

Havárie je mimořádná situace ohrožující chod síťové infrastruktury, organizace nebo důležitých IT služeb. Informace o havárii a případné nedostupnosti služeb zasílá zaměstnancům ICT technik. U havárie je nutné dbát na obecné zásady a minimalizaci škod a to především s ohledem na:

- a) ochranu zdraví;
- b) ochranu majetku;
- c) ochrana osobních údajů;
- d) ochranu dat.

#### **Odstranění havárie:**

Na odstranění havárie se podílí ICT technik. Zprovoznění důležitých a klíčových služeb se děje v pořadí důležitosti:

- a) Chod sítě a připojení do sítě internet;
- b) Informační systém;
- c) Telefony;
- d) Pošta;
- e) Vnitřní doménový systém;
- f) Souborové servery;
- g) E-learning;
- h) Další služby.

#### **Havárie služeb externích subjektů**

Telefony pevné linky:

- 1) Kontaktovat dodavatele a nahlásit poruchu operátorovi.
- 2) Spolupráce s dodavatelem na odstranění závady.







