

Zásady využívání ICT a přístupu k síti

Obchodní akademie a Střední odborná škola logistická, Opava, p.o.

Datum vydání:	30. 6. 2022
Verze:	1.0
Účinnost:	01. 9. 2022
Schválil:	Ing. Petr Kyjovský, ředitel školy

Obchodní akademie a Střední odborná škola logistická, Opava, příspěvková organizace
(dále jen škola)

vydává za účelem stanovení zásad využívání ICT a přístupu k síti dle standardů konektivity definované v Integrovaném regionálním operačním programu (IROP) tuto směrnici – Zásady využívání ICT a přístupu k síti dle standardu konektivity

Obsah:

1.	Použité termíny a zkratky	3
2.	Účel a cíl.....	3
3.	Rozsah působnosti	3
3.1	Základní ustanovení.....	4
3.2	Nadřízená dokumentace	4
3.3	Podřízená dokumentace	4
4.	Pravidla používání ICT.....	4
4.1	Povinnosti uživatele.....	4
4.2	Autentizace	4
4.3	Ochrana přístupu k prostředkům ICT	5
4.4	Ochrana autorských práv	5
4.5	Zakázaný obsah	5
4.6	Připojování zařízení do počítačové sítě	5
4.7	Technické zásahy do ICT a údržba.....	5
4.8	Přístup do Internetu	6
4.9	Detekce škodlivého SW	6
4.10	Monitorování provozu na síti	6
5.	Pravidla chování při práci v učebně s počítačovým vybavením.....	6
6.	Způsoby elektronické komunikace	7

1. Použité termíny a zkratky

ICT – informační a komunikační technologie

IROP – integrovaný regionální operační program

IS – informační systém

Informace – jakýkoli sdělitelný údaj textového, číselného, grafického či jiného charakteru v tištěné nebo elektronické podobě

Hardware – technické prostředky (dále též jen HW)

Software – programové prostředky (dále též jen SW)

Licence – oprávnění k užívání softwaru stanovené licenční smlouvou

Prostředky ICT – jsou servery, počítače (PC), jejich příslušenství a přídatná zařízení, přenosná paměťová média, počítačové sítě, telefony – jakož i další hardware a software

Server – řídicí počítač, na kterém běží vhodný síťový operační systém a který poskytuje stanicím a uživatelům přístup ke zdrojům sítě nebo k aplikacím

Síť – funkční celek zahrnující jeden nebo více serverů, terminály resp. stanice, technické prostředky propojení (aktivní a pasivní), přídatná zařízení, síťový operační systém a komunikační software Wi-Fi - bezdrátová síť

Administrátor (správce sítě) – zaměstnanec školy nebo smluvní dodavatel služby, který je ve škole zodpovědný za správu ICT, řešení požadavků a incidentů spojených s prostředky ICT

Uživatel – osoba, která je zaškolená a oprávněna k práci s prostředky ICT a aplikacemi

Škodlivý software – viry, malware, trojany, Adware, Backdoor, červ/worm, Spyware a další programy, které znemožňují, nebo zneprůjemňují práci PC, případně mohou svou činností způsobit ztrátu dat, poškození systému, zneužití výpočetní výkon nebo zapříčinit šíření jiného škodlivého SW

Přihlašovací jméno – řetězec znaků umožňující spolu s příslušným heslem přístup k ICT

Heslo – neveřejný řetězec znaků pro přístup k ICT

2. Účel a cíl

Účelem této směrnice je stanovení zásad využívání prostředků ICT a přístupu k síti dle standardů konektivity definované v Integrovaném regionálním operačním programu (IROP).

3. Rozsah působnosti

Směrnice je závazná pro všechny zaměstnance a žáky nebo studenty školy, externí dodavatele a další osoby (dále jen uživatelé), které v rámci plnění svých školních, pracovních a jiných povinností využívají informační a komunikační technologie školy. Tato směrnice musí být k dispozici všem uživatelům

prostředků ICT a počítačové sítě školy a tito jsou povinni se s ní seznámit. Toto seznámení potvrdí doložitelným způsobem.

3.1 Základní ustanovení

Prostředky ICT jsou veškeré prostředky školy, jejichž smysl je vytvářet, uchovávat, upravovat, vyměňovat, sdílet, vybírat, přenášet, používat či zpracovávat informace v elektronické podobě. ICT zahrnuje (ale neomezuje se pouze na tyto) prostředky:

- osobní počítače
- notebooky,
- mobilní zařízení
- servery
- periferní zařízení
- počítačová síť
- programové vybavení
- přístup k Internetu
- elektronická pošta
- kopírovací stroje
- telefonní linky, telefonní přístroje

Zneužívání ICT je posuzováno jako porušení školního řádu nebo pracovní smlouvy. Zneužití ICT může mít za následek disciplinární řízení (včetně ukončení pracovního poměru u zaměstnanců školy) a občanskoprávní nebo trestní zodpovědnost.

3.2 Nadřízená dokumentace

Školní řád.

3.3 Podřízená dokumentace

Není.

4. Pravidla používání ICT

4.1 Povinnosti uživatele

Uživatelé jsou povinni seznámit se s touto směrnicí a postupovat v souladu s jejím obsahem. Pokud k tomu není oprávněn, nesmí uživatel odesílat, přenášet nebo jakýmkoliv způsobem distribuovat informace a data.

4.2 Autentizace

Uživatelé se přihlašují přihlašovacím jménem a heslem podle pravidel a politik definovaných administrátorem. Stejně heslo nesmí mít uživatel nastaveno pro více různých systémů.

4.3 Ochrana přístupu k prostředkům ICT

Uživatelé nesmí bez oprávnění sdělovat jiným osobám nebo zaměstnancům školy, kteří k tomu nejsou oprávněni, kódy a jiné údaje umožňující přístup k jakýmkoliv prostředkům ICT (např. je zakázáno sdělovat hesla nebo přístupové kódy pro vzdálený přístup) a jsou povinni v maximální míře zabránit k přístupu k těmto údajům (nezapisovat je a nikde je neponechávat). Uživatelé jsou při opuštění zařízení povinni toto ochránit před neoprávněným přístupem (například uzamčením obrazovky).

4.4 Ochrana autorských práv

Uživatel je oprávněn používat k pracovním nebo studijním účelům jen SW, který je řádně licencován. Uživatelé nesmí pořizovat nelegální kopie materiálů, které jsou chráněny autorskými právy nebo zpřístupnit takové materiály ostatním ke kopírování. Uživatelé jsou zodpovědní za dodržování autorských práv a licenčních podmínek, které se vztahují k programům, souborům, grafice, dokumentům, audio a video souborům, zprávám a ostatním materiálům, které mají v úmyslu stahovat nebo kopírovat. Je zakázáno vyslovit souhlas s licenčními podmínkami nebo stahovat jakýkoliv materiál, za který se vybírají poplatky, bez předchozího doložitelného souhlasu administrátora.

4.5 Zakázaný obsah

Bez předchozího doložitelného souhlasu zaměstnavatele nebo administrátora nesmí být prostředky ICT používány k šíření, prohlížení nebo ukládání komerčních nebo osobních oznámení, žádostí a propagaci nesouvisejících s pracovním zařazením zaměstnance nebo plánem výuky žáka.

Mezi nepovolené úkony mimo jiné patří i hromadné rozesílání zpráv (spam), rozesílání hoax, rozesílání řetězových zpráv, hraní her, posílání a stahování velkých souborů, příjem a streaming audio a video souborů, poslech online rozhlasových stanic nebo jakákoliv jiná činnost, která vede k nadměrnému provozu na počítačové síti a **nesouvisí s pracovním nebo studijním využitím Internetu**. Je současně zakázáno tisknout materiály nesouvisejících s výukou nebo pracovní činností na prostředcích školy.

Je přísně zakázáno šíření, prohlížení a ukládání destruktivních kódů (jako jsou viry, apod.).

4.6 Připojování zařízení do počítačové sítě

Jakýkoliv prostředek ICT, připojující se do počítačové sítě školy musí být majetkem školy nebo zařízením schváleným administrátorem. Zařízení ve vlastnictví uživatelů se smí připojovat pouze k tomuto účelu vyhrazené síti (např. školní Wi-Fi oa-student / oa-host a podobně).

4.7 Technické zásahy do ICT a údržba

Zásahy do technického vybavení počítačů a jejich příslušenství může provádět pouze administrátor. Zásahy do ICT jsou uživatelům zakázány.

Všechna zařízení, za která je uživatel odpovědný, musí každý den před odchodem ze zaměstnání nebo z výuky vypnout, pokud není administrátorem stanoveno jinak.

4.8 Přístup do Internetu

Aby byla zajištěna bezpečnost a zabráněno šíření škodlivého SW v počítačové síti školy, mohou uživatelé přistupovat do Internetu pouze z počítačů připojených do počítačové sítě školy a musí tak činit pouze prostřednictvím schváleného bezpečnostního rozhraní. Obcházení zabezpečení počítačové sítě přímým přístupem do Internetu prostřednictvím mobilních přípojných bodů nebo jiným výslovně neschváleným způsobem je zakázáno mimo případ, kdy není a nebude použitý počítač připojen do školní počítačové sítě. Je nepřípustné při připojení ve školní síti mít současně aktivní připojení jednoho prostředku k jiné počítačové síti s přístupem do Internetu (např. mobilní přípojný bod).

Uživatelé Wifi oa-host provozované školou, jakkoliv není propojena se sítí školy, jsou rovněž povinni dbát bezpečnostních zásad a pravidel používání podle této směrnice.

4.9 Detekce škodlivého SW

Soubory získané ze zdrojů mimo školu, na discích, paměťových kartách a jiných přenosných médiích, soubory stažené z Internetu, získané z diskusních skupin a ostatních on-line služeb, soubory připojené k e-mailovým zprávám a z jiných neověřených zdrojů, mohou obsahovat škodlivý software, který může poškodit počítačovou síť školy. Uživatelé nesmí stahovat soubory z Internetu, včetně souborů získaných jako přílohu v e-mail zprávě od osoby zvenčí nebo použít přenosné médium z jiného než schváleného zdroje, aniž by nejdříve provedli detekci škodlivého SW v těchto materiálech a to pomocí administrátorem schváleného antivirového programu. Pokud má jakýkoli uživatel podezření na přítomnost škodlivého SW v počítačové síti, je povinen okamžitě informovat administrátora nebo vyučujícího.

4.10 Monitorování provozu na síti

Prostředky ICT jsou majetkem školy a smí být využívány pouze pro činnost školy. Škola má právo využívat programové a jiné vybavení, které umožňuje identifikovat a blokovat přístup k zdrojům v Internetu, které obsahují nebezpečné materiály nebo zakázaný obsah uvedený výše. Škola má dále právo logovat přístupy do počítačové sítě a monitorovat provoz a datové toky v rozsahu definovaném v aktuálně platném dokumentu Prokázání a kontrola naplnění standardu konektivity ve výzvách IROP (infrastruktura základních a středních škol) vydaného Ministerstvem pro místní rozvoj ČR.

5. Pravidla chování při práci v učebně s počítačovým vybavením

- a. Do odborné učebny žáci vstupují jen s doprovodem nebo se souhlasem vyučujícího
- b. Případné závady, které žák zjistí, nahlásí okamžitě vyučujícímu učiteli nebo administrátorovi (případně správci učebny, pokud je jmenován)
- c. Žáci se v učebně chovají tak, aby neohrozili své zdraví ani zdraví ostatních osob
- d. S vybavením učebny zacházejí všichni ohleduplně a používají je v souladu s touto směrnicí

- e. Žák pracuje u počítače pouze podle pokynů vyučujícího. Manipuluje pouze s klávesnicí, myší, dalším vybavením a programy, které zadal vyučující. Veškerá další manipulace se softwarem nebo hardwarem je zakázána.
- f. Při práci s počítačem je zakázáno používat vlastní paměťová média, SW, HW a další vybavení bez výslovného souhlasu vyučujícího
- g. Po ukončení práce žáci použité pomůcky vrátí na určené místo a uvedou počítač a pracovní místo do původního stavu. Za úklid pracovního místa a pomůcek zodpovídá vyučující
- h. Jídlo a nápoje je do učebny povoleno nosit jen s výslovným souhlasem vyučujícího.

6. Způsoby elektronické komunikace

Žáci komunikují s vyučujícími pomocí aplikace Bakaláři a pomocí školního e-mailového účtu.

Vyučující komunikují se zákonnými zástupci žáků pomocí nástroje Bakaláři a pomocí emailu, který je evidovaný v tomto systému.

Komunikace pracovníků sekretariátu s žáky probíhá pomocí emailu, který je žákům předán v prvním ročníku studia.

Při e-mailové komunikaci používají učitelé i žáci výhradně školní e-mailové účty. Žáci i učitelé a ostatní zaměstnanci školy jsou povinni zkontrolovat svůj školní email minimálně 1krát denně.