Táborské soukromé gymnázium a Základní škola s.r.o.

Směrnice upravující provoz informačních a komunikačních technologií na Táborském soukromém gymnázium a základní škole s.r.o.

ze dne 1.1.2019

č. 05/2019

Část I

Úvodní ustanovení

Čl. 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 „ICT“) na **Táborském soukromém gymnáziu a Základní škole** (dále jen „TSG a ZŠ “).
2) Příloha k této směrnici stanovuje pravidla uživatelské podpory, pohotovosti, komunikace a řešení havárií v oblasti ICT.
3) Tato směrnice je závazná pro všechny uživatele ICT TSG a ZŠ
4) Uživatelem ICT TSG a ZŠ je
   a) zaměstnanec TSG a ZŠ s platnou pracovní smlouvou, dohodou o provedení práce nebo dohodou o pracovní činnosti,
   b) pracovník na jiný typ smlouvy dle občanského nebo obchodního zákoníku, jehož práce je vykonávána prostřednictvím nebo s využitím ICT TSG a ZŠ,
   c) řádný žák školy
   d) další fyzická osoba s odůvodnitelným vztahem k TSG a ZŠ (zástupce dodavatele, účastník konference, student na výměnném pobytu apod.), jíž bylo povoleno na základě žádosti či uzavřené smlouvy využití ICT TSG a ZŠ.

Čl. 2

Základní pojmy

1) Hardware – souhrn technických prostředků výpočetní a komunikační techniky, jde především o počítače a jejich komponenty, periferie (tiskárny, monitory apod.) včetně jejich komponenty a prvky 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 VŠPJ.
5) Certifikát – elektronický dokument, kterým se prokazuje totožnost jeho držitele. 3
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 užít software stanoveným způsobem a ve stanoveném rozsahu.
8) Elektronický klíč, karta, čip – hardwarový prostředek (ISIC karta, přívěšek) sloužící k ověření totožnosti jeho držitele.
9) Pracovní stanice – osobní počítač včetně nezbytných periferií.
10) Notebook – přenosný osobní počítač.
11) Server – prostředek v počítačové sítí, který poskytuje služby klientům.
12) Klient – zařízení v počítačové síti, využívající služeb serveru.
13) DHCP (Dynamic Host Configuration Protocol) – protokol pro automatické přidělování IP adres jednotlivým osobním počítačům v počítačových sítích.
14) WIFI (Wireless Fidelity) – bezdrátové připojení k síti.
15) RFC (Request for Comments) – označení doporučených standardů.

16) DoS (Denial of Service) – typ útoku na přetížení služeb a serverů.
17) P2P (Peer-to-peer) – výměnné sítě, kde spolu komunikují klienti této sítě přímo.
18) IPv4 – Internet Protocol verze 4.
19) IPv6 – Internet Protocol verze 6.
20) Intranet – privátní počítačová síť, která je izolovaná od dalších vnějších sítí.
21) Doménové jméno (internetová/intranetová doména) - jednoznačné jméno (identifikátor) počítače nebo počítačové sítě, které jsou připojené do intranetu nebo internetu. Příkladem doménového jména je www.gtr.cz.
22) IS – informační systém TSG a ZŠ.
23) KICT – komise pro správu ICT

Část II
Nakládání s ICT majetkem TSG a ZŠ

Čl. 3
Pořízení, registrace a evidence

1) Pořízení ICT majetku probíhá v souladu se „Směrnicí o evidenci majetku TSG a ZŠ č. 01/2016“ v platném znění.
2) Hmotný a nehmotný ICT majetek je evidován spolu s ostatním majetkem v databázovém systému. Každý ICT majetek je zařazen do užívání pod unikátním inventárním číslem. Za sbírku skupiny určených inventárních položek zodpovídá určený pracovník – pedagog IVT.
3) Oproti písemnému potvrzení se předávají předměty, jejichž hodnota převyšuje 3000 Kč. Zaměstnanec odpovědný za hospodaření se svěřovanými předměty může rozhodnout o snížení hranice 3000 Kč. Převyšuje-li hodnota svěřeného předmětu 50 000 Kč, svěřuje se předmět vždy na základě dohody o odpovědnosti.
4) V případě vyřazení ICT majetku se k likvidačnímu protokolu přikládá vyjádření ICT technika školy nebo společnosti, zodpovědné za likvidaci ICT majetku, o nefunkčnosti tohoto majetku.
5) Předepsané revize a zkoušky počítačového hardware a audiovizuální techniky podle příslušné české technické normy zajišťuje správce budovy školy.

Část III
Uživatelé ICT TSG a ZŠ

Čl. 4
Obecné chování uživatelů

1) Uživatel ICT TSG a ZŠ se musí chovat tak, aby neporušoval platný právní řád České republiky a interní směrnice TSG a ZŠ.
2) Uživatel je povinen zejména
   a) hlásit bez prodlení vedoucímu KICT jakékoliv podezření na porušení této směrnice, závadné chování uživatelů ICT TSG a ZŠ (např. zneužití přístupu do sítě, podezření na nelegální činnost, odcizení či zneužití dat a hardware), závady hardware, podezření na nelegální software, chyby v softwaru či špatného fungování softwaru,
   b) využívat ICT TSG a ZŠ pouze pro vzdělávací, výchovnou, propagační činnost TSG a ZŠ, umělecké účely TSG a ZŠ, nebo úkoly související s provozem a správou TSG a ZŠ,

c) užívat k práci na pracovní stanici nebo notebooku ve vlastnictví TSG a ZŠ pouze legální software, který je určený pro jeho práci nebo studium a instalovaný pracovníky KI, nebo s jejich vědomím,
d) starat se o soukromá zařízení, která jsou připojena do sítě TSG a ZŠ. Mít je zabezpečená tak, aby nedocházelo k narušení bezpečnosti a omezování v provozu intranetu a internetu. V této souvislosti se vyžaduje instalace antivirové ochrany, firewall aj.
e) pravidelně číst (alespoň 1x za pracovní den) a v přiměřeném čase odpovídat na elektronickou poštu v e-mailové schránce TSG a ZŠ, byla-li mu zřízena.

3) Uživatel nesmí zejména

a) využívat ICT TSG a ZŠ k soukromým, komerčním nebo jiným účelům nesouvisejícím s činností TSG a ZŠ,
b) vystavovat prostředky ICT jakémukoliv nebezpečí,
c) zprostředkovat přístup k ICT TSG a ZŠ fyzickým či právnickým osobám, které nejsou uživateli ICT TSG a ZŠ
d) jakýmkoli způsobem poškozovat jakoukoli součást ICT TSG a ZŠ,
e) používat prostředky ICT v počítačové síti TSG a ZŠ, která nejsou v majetku TSG a ZŠ, s výjimkou zařízení připojených přes Wi-Fi, přenosných disků nebo pamětí, sluchátek s mikrofonem, fotoaparátů a kamer.
f) odstraňovat informace nebo označení identifikující autorská práva k software,
g) pracovat pod cizí identitou, používat prostředky k jejímu získání nebo zneužít v tomto pochybení či nedbalosti jiného uživatele,
h) sledovat nebo odposlouchávat provoz sítě s výjimkou oddělených laboratoří a to za předem stanovených podmínek,
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, DoS útoky nebo další softwarové nástroje),
j) zapojovat do sítě zařízení, která mohou ovlivnit komunikační provoz sítě (např. přepínače, směrovače aj.). KI toto může povolit ve výjimečných případech, ale u zapojení a nastavení musí být přítomen zaměstnanec školy,
k) na svých zařízeních v síti TSG a ZŠ 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 KI. Výjimku tvoří odpojení a připojení přenosných datových nosičů. Stěhování v rámci školy, jehož součástí je stěhování hardware, musí být předem konzultováno s KI a musí být definovány případné náklady a změny (potřeba změn v konfiguraci počítačové sítě aj.).

Čl. 5

Práce s přístupovými informacemi

1) Účet zaměstnance je zřízen na základě zadání uživatele do systému správcem sítě nebo členem KICT s touto pravomocí, obvykle správce informačního systému. Účet žáků je generován před nástupem do 1. ročníku 4letého, 6letého i 8letého studia a je zpravidla vydán při nástupu do školy. Účty dalších fyzických osob mohou být zřízeny na žádost zaměstnance TSG a ZŠ správci IS TSG a ZŠ. Součástí této žádosti musí být zdůvodnění žádosti a období, na jaké má být účet zřízen.

2) Uživatel je oprávněn používat pouze přidělený login a heslo. Login je vždy unikátní, daný správcem IS TSG a ZŠ a neměnný. Počáteční heslo je generováno a jeho převzetí je nutno podepsat. Uživatel je povinen udržovat heslo v tajnosti a neumisťovat písemnou formu na místo, které je dostupné dalším osobám.

3) Pomocí přiděleného loginu a hesla se přistupuje do elektronických aplikací TSG a ZŠ.

4) Přístup do dalších systémů vytváří určení členové KICT. Jde např. o informační systém Bakaláři, vnitřní informační systém „Spisovna“, knihovnický informační systém atd.

5) 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.

6) Účet zaměstnance je zrušen po zadání informace o ukončení právního vztahu k TSG a ZŠ do informačního systému TSG a ZŠ. Výjimky z tohoto pravidla povoluje vedoucí KICT. Účet žáka je převeden do režimu absolvent ihned po deaktivaci žáka kanceláří školy (vyřazení ze studia). Účty dalších fyzických osob jsou zrušeny ihned po skončení období, na které byly zřízeny. Povinností KICT je minimálně dvakrát za rok provádět kontrolu aktivních účtů, tj. zejména kontrolu obsahu ustanovení tohoto odstavce.

Čl. 6
Žáci školy

1) Žák užívá hardware a software školy pro účel, ke kterému je určen. Jde zejména o využívání počítačů, zařízení a aplikací pro studium a samostudium. Dále se jedná o kopírovací a tiskové služby a wifi.

2) Před opuštěním pracovní stanice TSG a ZŠ je žák povinen se odhlásit ze všech aplikací a operačního systému.

3) Žák není oprávněn se připojovat s vlastním zařízením do sítě TSG a ZŠ jinak než přes wifi.

4) Žák je povinen pro přidělení IP adresy u vlastního zařízení použít protokolu DHCP. Nastavení statické adresy je zakázáno.

5) Odpovědnost za své zařízení nese žák. Odpovídá především za zabezpečení zařízení (notebooky, notepady, telefony aj.), antivirovou ochranu a software. V případě zjištění problému s výše uvedenými body, je správce sítě oprávněn zařízení odpojit a vlastníkovi zaslat informační e-mail o důvodu odpojení. Po odstranění problému je možné přístup opět povolit.

6) Škola může poskytnout žákům software, který ze svého licenčního ujednání lze použít pro žáky a samostudium.

Čl. 7
Zaměstnanci

1) Základní zásady ochrany dat na pracovních stanicích a noteboocích (počítačích), které jsou ve vlastnictví TSG a ZŠ, jsou následující:

   a) Zaměstnanec je oprávněn využívat k práci pouze počítač, který byl k jeho práci určen (byl mu přidělen KICT) 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 TSG a ZŠ.
   c) Při opuštění učebny je každý zaměstnanec povinen se odhlásit ze systému počítače.
   d) 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.
   e) Šifrování dat a disků, pokud není řešeno ve spolupráci s KICT, není povoleno.
   f) Zaměstnanci školy mohou využívat své osobní počítače jen v případě, že splňují všechny podmínky bezpečného provozu (chráněn antivirem a používající pravidelné aktualizace systému), připojit je do sítě jen pře wifi nebo na místě k tomu určeném. Dále nesmí připojovat své osobní počítače do intranetu.

2) Pracovní stanice a notebooky zaměstnanců jsou všechny připojeny do internetu prostřednictvím počítačové sítě TSG a ZŠ. Výjimkou může být odůvodněné rozhodnutí nadřízeného pracovníka nebo odpojení pracovní stanice nebo notebooku z důvodu bezpečnosti.

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.

4) Zaměstnanci může vedoucí KICT povolit ve výjimečných případech přístup do monitoringu aplikací, do kterého mají práva přístupu pouze členové KICT. Musí se jednat o odůvodněný přístup vyplývající z pracovního zařazení zaměstnance.

Čl. 8
Komise pro správu ICT (KICT)

1) Členové KICT jsou oprávněni k přístupu ke všem pracovním stanicím a notebookům ve vlastnictví TSG a ZŠ a k datům na nich uloženým. Musí přitom dbát, aby jejich počínání bylo v souladu se zákonem na ochranu osobních údajů.

2) Členové KICT mají rozděleny kompetence, přístupy a správu ICT do skupin, a to vždy nejméně po 2 pracovnících. Přístupy a rozdělení kompetencí určuje vedoucí KICT v souladu s celkovou politikou bezpečnosti ICT TSG a ZŠ. Provoz sítě, aplikací a přístupu k nim může být monitorován. Priority řešení problémů určuje vedoucí komise.

3) Členové komise mají povinnosti zejména:

   a) Chránit zabezpečení ICT TSG a ZŠ.
   b) Chránit uživatelské a administrátorské přístupové údaje na servery, datová úložiště a do aplikací.
   c) Poskytovat uživatelskou podporu, konzultace a pomoc uživatelům.
   d) Nesdělovat přístupové informace na zařízení a aplikace školy třetím osobám, dodavatelům i dalším zaměstnancům KICT, kteří nemají provoz daného serveru nebo aplikace v kompetenci. V případě havárie nebo bezpečnostního incidentu je možné kompetence správy rozšířit i na další pracovníky KICT.
   e) 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.
   f) 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.
   g) Zajišťovat instalace učeben, laboratoří a pracovních stanic pro samostudium. Zajišťovat a kontrolovat přístupy do sítě TSG a ZŠ a vydávat přístupové čipy a karty.
   h) Zajišťovat chod kopírovacích zařízení a jejich vyúčtování pro zaměstnance a žáky TSG a ZŠ.
   i) Plnit další povinnosti vyplývající z interních řídících aktů TSG a ZŠ.

Část IV
Provoz na serverech a nakládání s daty

Čl. 9
Provoz na serverech

1) Poštovní server:

   a) Každý zaměstnanec nebo žák TSG a ZŠ má přidělen školní poštovní účet (e-mail).
   b) Přesměrování e-mailů mimo doménu gtr.cz není povoleno.
   c) KICT je povinna zveřejnit návod a poskytnout součinnost při nastavení e-mailových klientů uživatelů tak, aby uživatel mohl své e- maily číst v jednom e-mailovém klientovi.
   d) Velikost přílohy e-mailu je omezena na 20 MB

e) Systémově je zamezeno přijímat 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.
f) Pošta ve složce Nevyžádaná pošta starší 7 dnů je automaticky smazána.
g) Pošta ve složce Koš starší 30 dnů je automaticky smazána.

2) Souborový server:

a) Každý zaměstnanec nebo žák TSG a ZŠ má přiděleno diskové úložiště tzv. home.
b) Přístup do dalších umístění souborového serveru je dán pracovním nebo studijním zařazením.
c) Členové dané předmětové komise mají úplný přístup k souborům (právo editace textů) ve sdílené složce. Ostatní zaměstnanci mohou vložené soubory pouze číst.
d) Za obsah diskového úložiště (home) ručí vždy majitel účtu, za obsah na sdíleném diskovém uložišti 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.
e) Všechny soubory na serveru jsou zálohovány vždy při změně obsahu souboru. Je možné dohledat obsah určitého souboru před jeho poslední změnou.
f) KICT má právo na smazání obsahu složek home u žáků vždy po ukončení studia na TSG a ZŠ. Dva týdny před smazáním jsou uživatelé vždy upozorněni e-mailem. Smazané složky jsou zálohovány a data je možno obnovit na žádost zaslanou vedoucímu KICT, maximálně 30 dnů po smazání.

Čl. 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 TSG a ZŠ.

2) Uživatel je povinen zajistit ochranu dat před zneužitím a ztrátou. TSG a ZŠ 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 TSG a ZŠ oprávněno s daty nakládat, včetně možnosti a rozsahu jejich dalšího šíření. Nestanoví-li obecné závazné právní předpisy jinak, musí být tyto podmínky sjednány v písemné smlouvě. Smluvní ujednání musí být vždy připomínkováno ředitelkou školy, hospodářkou a vedoucím KICT.

4) Není-li si uživatel jist jakýmkoliv aspektem pořizování, zpracovávání, archivace a šíření dat, je povinen konzultovat problematiku s ředitelkou TSG a ZŠ.

Část V
Závěrečná ustanovení

Čl. 11
Porušení pravidel a sankce

1) Škody v rámci běžného užívání ICT majetku řeší „Směrnice o ochraně majetku TSG a ZŠ“.

2) 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.

3) 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 TSG a ZŠ.

4) Povinností uživatele ICT je hlásit vedoucímu KICT jakékoliv porušení či podezření na porušení pravidel (čl. 4, odst. 2, písm. a této směrnice). Povinností vedoucího KICT 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. 6, písm. a),
   b) zástupcem ředitelky školy, týká-li se porušení či podezření na porušení pravidel uživatele uvedeného v čl. 1, odst. 6, písm. b), c) a d),
   c) ředitelkou školy, nejedná-li se porušení či podezření na porušení pravidel na straně uživatele, nebo nelze-li původce porušení pravidel jednoznačně identifikovat.

Článek 12
Závěrečná ustanovení

1) Směrnice nabývá platnosti v den jejího podpisu a účinnosti dne 1. 1. 2019.
2) Směrnice bude zveřejněna v informačním systému TSG a ZŠ.

Tábor, 01.01.2019

……..
ředitelka školy