# ZNAKSKOL Střední odborná škola veterinární, mechanizační a zahradnická

 **a Jazyková škola s právem státní jazykové zkoušky**

 **České Budějovice, Rudolfovská 92**



### Organizační směrnice č. 8/2018

**o zásadách využívání ICT a přístupu k síti na SOŠ VMZ a JŠ**

**Účinnost od 27. srpna 2018**

České Budějovice 20. srpna 2018

 Ing. Bc. Břetislav Kábele

 ředitel školy

**1. Úvodní ustanovení**

Pravidla jsou platná pro všechny zaměstnance a studenty Střední odborné školy veterinární, mechanizační a zahradnické a Jazykové školy s právem stání jazykové zkoušky v Českých Budějovicích, zástupce externích subjektů a třetích stran, kteří spolupracují se školou. Cílem organizace bezpečnosti je vytvořit uvnitř školy takové vědomí potřeby bezpečnosti, které se stane neoddělitelnou součástí každodenního chodu školy.

**2. Základní pravidla**

Základní pravidla, která tvoří výchozí rámec pro řízení kvality služeb ICT:

- ICT může být na SOŠ VMZ a JŠ využívána pouze oprávněnými uživateli, a to jen pro plnění studijních, organizačních a pracovních úkolů, které plynou z pracovněprávního nebo studijního poměru k SOŠ VMZ a JŠ.

- uživatelé soukromých zařízení připojených do počítačové sítě SOŠ VMZ a JŠ či jinak využívající ICT školy jsou povinni dodržovat pravidla platící pro počítačové sítě SOŠ VMZ a JŠ, stejně tak jako všechny platné legislativní předpisy.

- používání elektronické pošty pro soukromé účely je tolerováno v rozumné míře tak, aby nijak neovlivnilo pracovní výkonnost zaměstnanců SOŠ VMZ a JŠ ani ICT školy pro elektronickou poštu, případně také funkčnost a výkonnost libovolné části informačního systému SOŠ VMZ a JŠ.

- využívání přístupu k internetu pro soukromé účely je tolerováno v rozumné míře tak, aby nijak neovlivnilo pracovní výkonnost zaměstnanců, studijní povinnosti žáků, kapacitu přístupového komunikačního kanálu, případně funkčnost a výkonnost libovolné části informačního systému SOŠ VMZ a JŠ.

- Na ICT provozované na SOŠ VMZ a JŠ smí být používán pouze legálně získaný software, a to jen za dodržování příslušných licenčních podmínek a doby platnosti tohoto softwaru. Totéž platí i pro zkušební používání softwaru (shareware, trialware apod.). Je zakázáno neoprávněné šíření nebo používání programů a dat, které jsou v rozporu s licenčními nebo jinými pravidly používání softwaru.

**3. Správa ICT SOŠ VMZ a JŠ**

- Správa ICT a současně celého informačního systému na SOŠ VMZ a JŠ zajišťují pověřené osoby, kterým jsou přiděleny jednotlivé úseky.

- Pověřené osoby mají právo podle potřeby vydávat provozní řády (např. provozní řád učebny, provozní řád laboratoře, provozní řád ICT domova mládeže atd.), který tato pravidla upřesňuje. Tyto dokumenty musí být v souladu se „Zásadami využívání ICT a přístupu k síti“.

- Pověřené osoby mají právo ve spolupráci s bezpečnostním manažerem SOŠ VMZ a JŠ monitorovat provoz zařízení. V případě porušování pravidel ze strany uživatele jsou povinni tomuto porušování zabránit. Pověřená osoba je při monitorování provozu povinna dodržovat všechna legislativní nařízení, která se na danou oblast vztahují včetně legislativních předpisů pro ochranu osobních dat a osobnosti uživatele.

- Pověření osoby mají právo po konzultaci s vedením školy stanovit harmonogram plánovaných výluk sítě. S tímto harmonogramem je povinen seznámit dotčené uživatele sítí.

- Pověřené osoby mají právo rozesílat e-mailové zprávy všem uživatelům sítě, pokud jde o mimořádně důležité a neodkladné sdělení.

**4. Práva a povinnosti uživatelů ICT**

Uživatelé ICT jsou povinni dodržovat následující pravidla:

- Hromadné e-mailové zprávy lze v nezbytném rozsahu rozesílat pouze za účelem plnění pracovních povinností, a to jen okruhu příjemců, kterým daná zpráva náleží.

- Uživatel nesmí používat jakékoli neoprávněně získané licenční klíče, kódy a hesla, či jiné prostředky sloužící k obcházení zajištění informační bezpečnosti a ochrany počítačových programů.

- Uživateli je zakázáno odstranit jakékoli informace, označení či zařízení identifikující nositele či vykonavatele autorských práv k počítačovým programům a datům podléhajícím autorskému zákonu.

- Uživatel je povinen umožnit kontrolu zařízení vykonávanou pověřenou osobou. Nesmí vytvářet nebo pozměňovat data s cílem ovlivnit (mást) kontrolu oprávněnosti použití počítačových programů. Není povoleno jakkoli bránit v kontrole vybavení ICT.

- Informační systém SOŠ VMZ a JŠ pro elektronickou poštu musí být využíván v souladu s platnými normami. Nesmí být zneužit proti zájmům SOŠ VMZ a JŠ a České Republiky, ani používán k soukromým podnikatelským aktivitám zaměstnanců a žáků. Dále je přísně zakázáno využívat elektronické pošty k šíření jakýkoliv pomlouvačných, urážlivých, obscénních, či výhružných materiálů, k šíření násilí, rasizmu, nesnášenlivosti, fašismu, xenofobie, pornografie, k propagaci politických názorů, hnutí a skupin směřujících k potlačení práv a svobod občanů a k šíření reklamních zpráv.

- Přístup k informačnímu nebo internetu (včetně sociálních sítí) nesmí být zneužit proti zájmům SOŠ VMZ a JŠ a České Republiky, ani používán k soukromým podnikatelským aktivitám zaměstnanců a žáků. Dále je přísně zakázáno využívat připojení k celosvětové počítačové síti internet za účelem šíření jakýkoliv pomlouvačných, urážlivých, obscénních, či výhružných materiálů, k šíření násilí, rasizmu, nesnášenlivosti, fašismu, xenofobie, pornografie, k propagaci politických názorů, hnutí a skupin směřujících k potlačení práv a svobod občanů a k šíření reklamních zpráv.

**5. Přístupová práva uživatelů k informačním systémům SOŠ VMZ a JŠ**

- Přístup k ICT a datům SOŠ VMZ a JŠ musí být přidělován dle principu „přístup pouze tam, kde je to nezbytné“.

- Každý uživatel se hlásí k informačním systémům na základě svého uživatelského účtu, který je chráněn uživatelským jménem a heslem. Daný účet má přiřazeny předdefinované sady oprávnění dle uživatelovy pracovní náplně nebo potřeb pro výuku.

- Přístup musí být schválen odpovědnými osobami. Nastavení konkrétních přístupových práv zajištují určení pracovníci.

- Uživatel může požádat o změnu přístupových práv ke službám sítě internet nebo k informačním systémům školy na základě žádosti schválené nadřízeným pracovníkem.

- Zablokování a zrušení přístupu ke službám sítě internet nebo k informačním systémům školy při odchodu zaměstnance nebo žáka se vykoná na základě rozhodnutí vedení školy.

- Uživatel má právo používat informační systémy SOŠ VMZ a JŠ včetně služeb počítačové sítě v rámci svých přístupových práv. Rozsah práv používání informačních systémů pro uživatele je určován členy vedení školy a je přidělován pověřenou osobou v závislosti na pracovním zařazení či studijních parametrech. Tato oprávnění mohou být také dočasná.

- Každý uživatel, který chce užívat služeb informačních systémů SOŠ VMZ a JŠ, musí být registrován a musí být známa jeho identita (totožnost osoby).

- Přístup uživatele k počítačové síti SOŠ VMZ a JŠ musí být vždy chráněn dostatečně silným heslem.

**6. Povinnosti uživatelů informačních systémů SOŠ VMZ a JŠ ve vztahu k ochraně přístupových hesel**

Uživatele se při tvorbě hesel musí řídit pravidly, která zajišťují používání kvalitních hesel.

- Hesla nesmí být jakýmkoliv způsobem sdělena jiné osobě.

- Hesla nesmí být nikde poznamenána a musí se udržovat v tajnosti.

- Nesmí být jakkoliv umožněno jiné osobě seznámit se s heslem.

- Jako hesla nesmí být použita jména blízkých osob, zvířat a další slova, která mohou být odhadnuta ze znalosti držitele hesla.

- Nesmí být použito heslo, obsahující stejné nebo po sobě jdoucí znaky (např. 111, aaa, 1234, qwert).

- Heslo musí být dostatečně silné, tak aby se nedalo jednoduše strojově nebo ručně prolomit (ideálně kombinace malých a velkých písmen a číslic, délka alespoň 6 znaků). Mělo by být pravidelně měněno v závislosti na rizicích spojených s prolomením.

- Hesla nesmí být zaznamenána na papíře nebo v obdobné podobě (výjimku tvoří bezpečné uložení administrátorských hesel pro případ havárie nebo nepředvídatelné okolnosti).

- Hesla se musí změnit v případě jakéhokoliv náznaku možného kompromitování systému nebo hesla.

- Uživatel si změní své heslo při prvním přihlášení do informačního systému SOŠ VMZ a JŠ.

- Uživatel nese zodpovědnost za prozrazení jeho hesla a následné zneužití svého účtu v rámci SOŠ VMZ a JŠ.

**7. Povinnosti uživatelů informačních systémů SOŠ VMZ a JŠ ve vztahu k ochraně ICT**

- Uživatelé jsou povinni zajistit bezpečnost neobsluhovaných uživatelských zařízení, a to zejména pracovních stanic, kdy se v případě ukončení nebo přerušení práce a odchodu z pracoviště musí odhlásit, případně uzamknout pracovní stanici.

- Žáci jsou povinni, po ukončení výuky v učebně, se odhlásit nebo vypnout pracovní stanici.

- Pokud uživatel záměrně nebo svou nedbalostí umožní využívání ICT jiné osobě, je plně zodpovědný za následky a škody s tím vzniklé.

- Uživatel IS SOŠ VMZ a JŠ nesmí záměrně nebo bez závažného důvodu přetěžovat počítačovou síť nebo se snažit získat neoprávněný přístup k informacím, datům nebo přístupovým údajům jiných účastníků. Pokud uživatel zjistí, že přístup k takovým údajům má, je povinen tuto skutečnost neprodleně oznámit pověřené osobě pro správu informačních systémů.

**8. Povinnosti uživatelů informačních systémů SOŠ VMZ a JŠ při bezpečnostním incidentu**

Bezpečnostní incident je definován jako porušení bezpečnosti systému, kdy je v rozporu s bezpečnostní politikou získán přístup k informacím nebo zdrojům systému.

- V případě důvodného podezření na vznik bezpečnostního incidentu přeruší koncový uživatel neprodleně práci a informuje pověřenou osobu nebo vedoucího zaměstnance.

- Další činnosti podřídí uživatel informačních systémů SOŠ VMZ a JŠ pokynům vedoucího pracovníka nebo pověřené osoby.

- Podnikat jakékoliv kroky ke zjištění příčin incidentu nebo k jeho omezení je koncovým uživatelům zakázáno. Výjimkou je, pokud hrozí nárůst škod na majetku (movitém i nemovitém), nebo je-li ohroženo zdraví osob.

**9. Datová síť SOŠ VMZ a JŠ**

Provozní pravidla datové sítě SOŠ VMZ a JŠ:

- Veškerá nastavení nebo instalaci kabeláže či zařízení v síti SOŠ VMZ a JŠ může provádět pouze pověřená osoba.

- Pověřená osoba vede patřičnou dokumentaci o topologii, zařízeních a nastavení těchto zařízení v síti.

- Uživateli není dovoleno provádět sledování provozu sítě nebo činnosti vedoucí k omezení provozu na síti.

- Pověřená osoba může odpojit taková zařízení, která negativně ovlivňují chod ostatních zařízení, nebo jejichž provoz je v rozporu s těmito pravidly. Pověřená osoba neprodleně informuje o odpojení daného uživatele odpovědného za chod zařízení.

- Pokud pověřená osoba nemůže odpojit konkrétní zařízení omezující chod sítě, může ve výjimečných případech odpojit segment nebo část segmentu sítě.

**10. Připojení koncových zařízení do sítě SOŠ VMZ a JŠ**

Obecná pravidla připojování zařízení do sítě SOŠ VMZ a JŠ:

- Instalaci koncového zařízení (které je v majetku školy) a jeho připojení do počítačové sítě provádí pověřená osoba.

- Každé zařízení je evidování v centrální evidenci SOŠ VMZ a JŠ a to včetně programového a technického vybavení v rámci všech zákonných nařízení ČR.

- Každé zařízení připojené do počítačové sítě SOŠ VMZ a JŠ musí splňovat požadavky pro bezproblémový provoz (vhodný antivirový program, osobní firewall, záplaty, aktualizace…)

- Není povoleno zařízení nebo jeho části přemisťovat bez vědomí pověřené osoby, pokud k tomu nejsou závažné důvody (ohrožení života, zdraví či majetku).

- Uživatel je povinen udržovat zařízení způsobem daným výrobcem nebo pověřenou osobou, předcházet možnému poškození, zničení a ztrátě. Veškeré nákupy koncových zařízení musí být předem schváleny pověřenou osobou, vedoucím pracovníkem, vedoucím ekonomického úseku a ředitelem školy.

- Při nákupu koncových zařízení musí pověřená osoba zajistit kompatibilitu se stávající hardwarovou a softwarovou strukturou.

- Programové vybavení může na koncové zařízení instalovat pouze pověřená osoba a ta pouze v případě platné licence pro daný software. Doklady o nabytí veškerého programového vybavení používaného na SOŠ VMZ a JŠ musí být řádně evidovány.

**11. Uživatelská koncová zařízení**

Obecná pravidla připojování uživatelských koncových zařízení do sítě SOŠ VMZ a JŠ:

- Každé koncové zařízení má určenou osobu (správce), která zodpovídá za provoz a stav zařízení.

- Každý uživatel je zodpovědný za svou činnost na tomto zařízení nebo činnost provozovanou jeho prostřednictvím.

- Pokud koncové zařízení využívá více uživatelů současně, musí být zjištěna autorizace každého z nich tak, aby bylo vždy možné identifikovat konkrétního uživatele v daném čase.

- veškeré instalace, opravy (mimo běžnou údržbu) a administrace koncového zařízení je oprávněna provádět pouze pověřená osoba.

- Uživatel nesmí zasahovat do programů, dat a technického vybavení počítačové sítě. Jsou zakázány jakékoli změny konfigurace počítačů či jiných prostředků, které by mohly mít vliv na provoz počítačové sítě.

- Je možno udělit oprávnění k administraci počítače. V takové případu, je uživatel zodpovědný za veškeré programové vybavení, které nebylo instalováno pověřenou osobou. Uživatel musí zároveň evidovat oprávněnost využívání nainstalovaných programů.

- V případě poruchy nebo problémů se zařízením uvede problém písemně do knihy závad a požadavků, která je umístěna na sekretariátu školy. Kromě záznamu do knihy může zároveň přímo kontaktovat pověřenou osobu, se kterou si domluví další postup. Pověřená osoba požadavek vyřeší v rámci svých stanovených hodin na údržbu a opravy.

- Za data uložená na koncové stanici je zodpovědný vlastník dat, tj. osoba, která je na toto zařízení uložila nebo modifikovala.

**12. Koncová serverová zařízení**

- Vedení školy určuje podmínky připojení koncového serverového zařízení a jeho provoz. Veškeré nákupy síťových a serverových zařízení schvaluje vedoucí ekonomického úseku a ředitel školy.

- Správu zařízení zajišťuje pověřená osoba, na kterou mohou být delegována příslušná práva na administraci zařízení. V takovém případě je pověřená osoba zodpovědná za provoz zařízení.

- Za data uložená na serverových zařízeních je zodpovědný vlastník dat, tj. osoba, která je na toto zařízení uložila nebo modifikovala.

**13. Přidělování doménových názvů v síti SOŠ VMZ a JŠ**

Obecná pravidla přidělování doménových názvů:

- Pravidla se vztahují na všechny názvy nebo na všechny rozsahy IP adres přidělené síti SOŠ VMZ a JŠ.

- Správu všech doménových záznamů pro SOŠ VMZ a JŠ vede pověřená osoba. Pověřená osoba provádí změny v souladu s níže uvedenými pravidly.

- Základním doménovým názvem pro SOŠ VMZ a JŠ je název druhé úrovně, tj. „soscb.cz“. Další používaná doménová jména (vázané na stejnou IP adresu) jsou: „sosvaz.cz“.

**14. Standardy pro informační systémy – obecná pravidla**

- Hospodářka školy vede evidenci veškerých informačních systémů na SOŠ VMZ a JŠ a to jak hardware, tak i software.

- Vývoj a další rozvoj informačního systému je uskutečňován formou požadavků pověřených osob, které musí být vždy schváleny vedením školy.

- Připomínky v rámci provozu informačního systému jsou předávány pomocí pověřených osob administrativnímu správci.

- Administrativní správce je odpovědný za správu a provoz informačního systému a komunikaci s dodavateli. Administrativní správce provádí dále zejména následující činnosti:

 - přiděluje přístupová práva do informačního systému

- provádí správu serverových aplikací, školení a podporu uživatelům informačního systému

 - spravuje datový obsah informačního systému

 - spravuje webové prezentace informační systému

 - zajišťuje podklady pro rozvoj informačního systému

- Technický správce je osoba zodpovědná za provozuschopnost informačních systémů, instalaci, správu a konfiguraci software a hardware. Na škole je jako technický správce určena pověřená osoba pověřené osoby).

- Webová prezentace – je internetová forma zveřejnění informací o SOŠ VMZ a JŠ nebo její části. Technickým správcem všech oficiálních webových prezentací zadaných členy vedení SOŠ VMZ a JŠ je administrativní pracovník. Jiné webové prezentace než oficiální prezentace SOŠ VMZ a JŠ, s výjimkou osobních webových prezentací zaměstnanců, nejsou povoleny. Veškeré webové prezentace podléhají schvalování vedením školy.

- Osobní webová prezentace – je prezentace konkrétního uživatele ICT SOŠ VMZ a JŠ, umístěné na serverech SOŠ VMZ a JŠ v Českých Budějovicích s veřejnou adresou https://www.soscb.cz/uživatelské\_jméno. Za administrátora, správce a osobu odpovědnou za data v rámci této prezentace je považován uživatel ICT, kterému byla webová prezentace zřízena a povolena.

**15. Oblasti působení informačních systémů SOŠ VMZ a JŠ**

- Oblast studijní – zahrnuje veškeré informační systémy, které se používají pro podporu vzdělávacího procesu na SOŠ VMZ a JŠ. Stěžejním systémem je studijní informační systém – Systém agent pro školy (SAS). Dalšími systémy jsou tzv. „Podpora výuky“ – portál, kde jsou vystaveny podpůrné materiály pro jednotlivé vyučované předměty a systém Moodle - systém pro tvorbu výukových systémů a elektronických kurzů na internetu.

Pro vyhledávání odborné literatury ve školní knihovně je k dispozici systém CLAVIUS (databáze obsahující všechny knižní tituly, které je možno si zapůjčit ve školní knihovně).

- Oblast provozní – zahrnuje veškeré informační systémy podporující chod školy v provozní oblasti. Jedná se o ekonomicky, personální, mzdový a jídelní informační systém. Tyto informační systémy jsou výhradně centralizované.

**Zásady užití ICT pro zaměstnance SOŠ VMZ A JŠ České Budějovice – vybrané body**

Škola je stání odbornou institucí, které zodpovídá za ochranu žáků.

Všichni její zaměstnanci musí přijmout veškerá možná a nezbytná opatření k ochraně dat a informačních systémů školy před zneužitím, zavirováním, neoprávněným přístupem, poškozením, ztrátou či zcizením. Nedílnou součástí těchto vytažených nejdůležitějších zásad je směrnice „Zásady využívání ICT a přístupu k síti na SOŠ VMZ a JŠ“. Používání ICT by mělo být v souladu se školním řádem, se směrnicí „Zásady využívání ICT a přístupu k síti“ a platnou legislativou ČR.

- Školní informační systém budu užívat správně a dle platné legislativy ČR. Vím, že trestní zákoník definuje podstatu řady trestných činů v rámci ICT např.:

 - získání neoprávněného přístupu k hardwarovému nebo softwarovému vybavení

 - získání takového materiálu a úmyslem spáchat trestný čin

 - získání takového materiálu a úmyslem usnadnit páchání trestného činu

 - nezákonná úprava počítačového materiálu

 - neoprávněný vstup do databáze

 - neoprávněná změna dat v databázi

 - apod.

- Rozumím, že hardware a software dostupný na mém pracovišti může být užíván pouze zaměstnanci SOŠ VMZ a JŠ a to jen pro vzdělávací a pracovní účely s výjimkou bodu 2 směrnice „Zásady využívání ICT a přístupu k síti na SOŠ VMZ a JŠ“

- Nebudu nechávat informační systém bez odhlášení se ze systému nebo náležitého uzamčení přístupu heslem.

- Budu respektovat bezpečnost systému a nebudu zveřejňovat heslo či informace o zabezpečení.

- Budu používat silné heslo (ideálně kombinace malých a velkých písmen a číslic, délka alespoň 6 znaků)

- Nebudu se pokoušet instalovat zakoupený či stažený software včetně lišt vyhledávače nebo hardwaru bez souhlasu pověřené osoby.

- Zajistím, že veškeré osobní údaje žáků, zaměstnanců, rodičů (zákonných zástupců) budou uchovávány v souladu se Zákonem o ochraně osobních údajů.

- Veškeré osobní údaje budou získávány a zpracovány řádně zákonným způsobem, uchovávány pouze pro specifické účely a po dobu nezbytně nutnou.

- Obrázky a videa žáků budou použity pouze v souladu se školním řádem a vždy s ohledem na informovaný souhlas rodičů (zákonných zástupců) nebo plnoletých žáků.

- Nebudu uchovávat pracovní dokumenty, které obsahují citlivé nebo osobní údaje související se školou (včetně obrázků, souborů, videí atd.) na žádném osobním zařízení, pokud není zabezpečené nebo zašifrované.

- Budu chránit zařízení v mé péči před neoprávněným přístupem nebo krádeží.

- Nebudu ukládat do školního informačního systému žádné osobní informace, které nesouvisí s činností školy (**osobní fotografie, soubory, finanční informace…**)

- Budu respektovat autorská práva a práva duševního vlastnictví.

- Budu okamžitě hlásit veškeré incidenty týkající se bezpečnosti žáků na internetu výchovnému poradci.

- Nebudu se pokoušet obejít filtrování ani zabezpečení sítě zavedené školou.

- Moje elektronická komunikace s žáky, rodiči, zákonnými zástupci a dalšími odborníky se uskutečňuje přes školní e-mail, telefon nebo datovou schránkou.

- Nebudu vytvářet, přenášet, zobrazovat, publikovat nebo šířit jakýkoli materiál, který by mohl obtěžovat nebo působit nepříjemnosti jakékoli osobě.

- Chápu, že mé využívání informačních systémů, internetu a e-mailů může být sledováno a zaznamenáváno, aby se zajistila shoda s pravidly.

Škola může uplatnit své právo na kontrolu využívání informačních systémů SOŠ VMZ a JŠ včetně přístupu k internetu a e-mailů s cílem sledování dodržování těchto zásad přijatelného užití a školních pravidel ochrany dat.

V případě podezření na neoprávněné a nevhodné užívání služeb informačního systému nebo nepřijatelného či nevhodného chování, zahájí škola disciplinární řízení, a to ve shodě s Pracovním řádem, Školním řádem, Zákoníkem práce a Trestním zákoníkem – v platném znění.

Má-li škola podezření, že je sytém zneužíván pro páchání trestné činnosti či k ukládání protiprávních textů, obrazových či zvukových záznamů, předloží záležitost odpovědným orgánům činným v trestním řízení.

**Přečetl(a) jsem a porozuměl(a) jsem, souhlasím a budu dodržovat zásady přijatelného užití ICT pro zaměstnance.**

**Jméno Podpis**

**Jméno Podpis**

**Jméno Podpis**

**Jméno Podpis**