

Vysoká škola zdravotnická, o. p. s.



SMĚRNICE ŘEDITELE č. 1/2015

Pravidla užívání počítačových sítí a provozování programového vybavení

Článek 1.

Úvodní ustanovení

- 1.1. VŠZ provozuje vnitřní počítačovou síť pro zabezpečení svých elektronických komunikačních potřeb (dále jen „počítačová síť VŠZ“).
- 1.2. Počítačová síť VŠZ je ve vlastnictví VŠZ a je provozována pro podporu vzdělávací, vědecké, výzkumné, vývojové, inovační, umělecké nebo další tvůrčí činnosti, a dále pro zajištění provozu a správy VŠZ, v souladu s činností VŠZ danou zákonem č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a vnitřními předpisy a normami VŠZ. Účelem počítačové sítě VŠZ je datové propojení koncových uživatelů za účelem přístupu k elektronickým komunikačním službám a digitálním datovým zdrojům.

Článek 2.

- 2.1. Tento vnitřní předpis stanovuje základní pravidla provozu počítačové sítě VŠZ pro zajištění jejího efektivního a bezpečného využívání a stanovuje práva a povinnosti uživatelů této sítě VŠZ.
- 2.2. Provozní technické pokyny pro užívání počítačové sítě VŠZ a provozování programového vybavení VŠZ jsou umístěny na webové stránce <http://www.vsdrav.cz/cz/vsdrav/dokumenty> a jsou průběžně aktualizovány.

Článek 3.

Organizační struktura počítačové sítě VŠZ a její správa

- 3.1. Počítačová síť VŠZ se skládá ze dvou lokalit – Praha a Vsetín.
- 3.2. K počítačové síti VŠZ jsou připojeny servery a koncová uživatelská zařízení (počítače, tiskárny, mobilní a další elektronická zařízení).
- 3.3. Připojením k síti, pro účely tohoto vnitřního předpisu, se rozumí přímé i nepřímé připojení uživatelského zařízení k počítačové síti VŠZ.
- 3.4. Každému připojenému uživatelskému zařízení je přidělena jedinečná síťová adresa (dále jen „IP adresa“), a to buď z veřejného, nebo z neveřejného rozsahu.
- 3.5. Uživatelem počítačové sítě VŠZ (dále též „uživatel“ nebo „koncový uživatel“) je každý, kdo užívá počítače nebo jiná koncová zařízení, včetně programového vybavení, přímo nebo nepřímo připojené k počítačové síti VŠZ.
- 3.6. Správu a rozvoj služeb páteřní počítačové sítě a správu centrálních serverů, umístěných v datových centrech VŠZ, zajišťuje Správce sítě.

- 3.7. Součástí VŠZ si mohou zajišťovat další zaměstnance podle svých potřeb, zejména na správu serverů určených pro vlastní aplikace podporující hlavní a doplňkovou činnost, které nejsou zařazeny ve struktuře školních informačních systémů. Tito zaměstnanci koordinují svou činnost se Správcem sítě.
- 3.8. V případě poruchy na počítačové síti VŠZ má Správce sítě právo odpojit segment sítě, který způsobuje problémy, na nezbytně nutnou dobu, aby byla zachována funkčnost zbylé části sítě.

Článek 4. Článek 3 **Programové vybavení**

- 4.1. Operační systémy a další programového vybavení spravuje Správce sítě.
- 4.2. Uživatel má právo používat pouze programové vybavení schválené Správcem sítě. Kopírovat programy lze pouze při dodržení zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „autorský zákon“), a licenčních podmínek. Kopírování zároveň musí být prováděno s vědomím Správce sítě. Při používání neschválených programů uživatel plně odpovídá za případné škody, které těmito programy způsobí.
- 4.3. Uživatel není oprávněn instalovat programové vybavení na zařízení v majetku VŠZ, které je připojené k počítačové síti VŠZ v učebnách nebo jiných výukových a veřejně přístupných prostorách a v laboratořích. V ostatních případech za instalaci a činnost programového vybavení, jehož instalace proběhla bez účasti Správce sítě, plně odpovídá uživatel.
- 4.4. Uživatel nesmí provést změnu konfigurace počítače nebo jakéhokoli jiného koncového zařízení nebo počítačové sítě VŠZ. V případě nedodržení tohoto pravidla má Správce sítě právo odpojit nežádoucí zařízení, část sítě nebo uživatele. Za zvláště hrubé porušení pravidel se považuje takový vědomý zásah do počítače nebo jiného zařízení, nebo jejich programových vybavení, který vede k jeho zhroucení, poruše či nežádoucímu chování. Za škody způsobené porušením tohoto bodu nese uživatel plnou zodpovědnost.

Článek 5. **Práva a povinnosti uživatelů a jejich identita**

- 5.1. Zaměstnanci a studenti VŠZ mají oprávnění stát se uživatelem počítačové sítě VŠZ. Využívání počítačové sítě VŠZ jinými osobami je možné pouze na základě svolení vydaného rektorem VŠZ nebo ředitelem VŠZ a s vědomím Správce sítě.
- 5.2. Každý uživatel počítačové sítě VŠZ je povinen seznámit se s pravidly obsaženými v tomto vnitřním předpisu, s pokyny obsaženými na webové stránce <http://www.vszdrav.cz/cz/vszdrav/dokumenty/>. Pokud je pro přístup k počítačové síti VŠZ vyžadována identita uživatele, je uživatel povinen používat ze strany VŠZ přidělené uživatelské jméno. Uživatel je povinen používat pro ověření identity netriviální heslo o minimální délce 8 znaků obsahující alespoň jedno malé písmeno, jedno velké písmeno a jednu číslici. Nepřípustné je hesla kamkoliv zapisovat.
- 5.3. Přístupová práva uživatele k počítačové síti VŠZ a k programovým modulům (dále též jako „uživatelská práva“) jsou přidělena Správcem sítě. Uživatel není oprávněn získávat jakýmkoliv prostředky přístupová práva, která mu nebyla přidělena. Pokud uživatel získá jemu nepřislušející přístupová práva, je povinen tuto skutečnost neprodleně oznámit příslušnému Správci sítě a tato práva nesmí použít.
- 5.4. Uživatelům počítačové sítě VŠZ se zakazuje:

- a) poskytnout své přidělené uživatelské jméno a heslo jiné osobě,
 - b) zneužít nedbalosti jiného uživatele (například jeho neodhlášení od koncových zařízení) k činnosti pod cizí identitou,
 - c) provádět jakékoli akce směřující ke zjištění hesla jiného uživatele,
 - d) zneužívat počítačovou síť VŠZ k získávání neautorizovaných přístupových práv (zejména překračujících rozsah licence) k informačním zdrojům, které jsou dostupné prostřednictvím počítačové sítě VŠZ,
 - e) poskytnout ve své působnosti ze zařízení jimi vlastněných, najatých, vypůjčených či provozovaných konektivitu a/nebo možnost zneužití informačních zdrojů počítačové sítě VŠZ třetí osobě,
 - f) zasahovat do programového a technického vybavení počítačové sítě VŠZ bez souhlasu příslušného správce; explicitně nesmí provést takové neautorizované změny konfigurace počítačů či jiných koncových zařízení,
 - g) využívat počítačovou síť VŠZ pro své soukromé nebo komerční aktivity,
 - h) vědomě i nevědomě narušovat práci ostatních uživatelů, provoz a výkonnost počítačové sítě VŠZ,
 - i) používat služby či programové prostředky, které ohrožují činnost počítačové sítě VŠZ nebo ji nadměrně zatěžují,
 - j) vydávat se za jiného či anonymního uživatele (vyjma služeb, které anonymitu připouštějí – např. web) nebo libovolným způsobem falšovat vlastní identitu,
 - k) vytvářet nedovolené kopie cizích dat a provádět odposlech provozu v počítačové síti VŠZ za účelem získání cizích dat
 - l) při odchodu od pracoviště počítač nechávat přihlášený nebo vypnutý. Požadovaný stav je obrazovka vyzývající k přihlášení.
 - m) připojovat se do sítě VŠZ pomocí VPN prostřednictvím zařízení, které není aktualizované, nemá aktivní antivirovou ochranu a je zdrojem podezřelé aktivity. Za škody způsobené těmito zařízeními nese zodpovědnost uživatel.
 - n) otevírat emailové zprávy nebo jejich přílohy, které vykazují znaky podvodného jednání. Pokud si uživatel není jistý legitimitou emailové zprávy, před jejím otevřením ji musí zkontrolovat se Správcem sítě. Uživatel plně zodpovídá za škody, které otevíráním podezřelých zpráv bez vědomí Správce sítě způsobí.
- 5.5. Uživatelé jsou povinni bez prodlení uposlechnout dalších pokynů Správce sítě a respektovat administrativní opatření regulující přístup k užívaným technickým prostředkům počítačové sítě VŠZ.
- 5.6. Uživatelé jsou povinni sledovat a bezpodmínečně dodržovat veškeré provozní pokyny Správce sítě sdělované jak přímo, tak uveřejněním na stránkách <http://www.vszdrav.cz/cz/vszdrav/dokumenty/>, a to na všech koncových zařízeních, která používají.
- 5.7. Správce sítě je oprávněn dodatečně reagovat na aktuální situaci provozními pokyny, které nejsou v rozporu s těmito pravidly.
- 5.8. Uživatelé jsou dále povinni v rámci svých uživatelských práv v maximální možné míře zabezpečit svá data proti zneužití třetími osobami.
- 5.9. VŠZ neodpovídá za ztrátu uživatelských dat uložených mimo síťové úložiště. Za pořizování záložních kopií vlastních uživatelských dat a odpovídají uživatelé sami.
- 5.10. Uživatel nese odpovědnost za obsah vlastních veřejně dostupných webových stránek a jiných soukromých informačních zdrojů, zejména pak za porušení autorského zákona či dalších obecně závazných právních předpisů, při využívání materiálů jiných právnických nebo fyzických osob.

- 5.11. Uživatelé mají právo na ochranu osobních údajů a soukromí, a to i v případě, kdy svá soukromá data nechrání. Uživatel nesmí zneužívat cizích dat v uživatelských adresářích a systémových schránkách elektronické pošty.

Článek 6.

Připojení zařízení k počítačové síti VŠZ prostřednictvím pevných přípojek

- 6.1. Připojování a odpojování koncových zařízení k počítačové síti VŠZ prostřednictvím pevných přípojek nebo změnu jejich síťové konfigurace provádí Správce sítě.
- 6.2. Každému připojenému koncovému zařízení je přidělena IP adresa (automaticky nebo staticky). IP adresa nesmí být uživatelem měněna.

Článek 7.

Připojení zařízení prostřednictvím bezdrátové sítě, pevných přípojek na veřejných místech a připojení soukromými prostředky

- 7.1. Při připojení zařízení k počítačové síti VŠZ prostřednictvím bezdrátové sítě, pevných přípojek na veřejných místech nebo připojení soukromými prostředky je uživatel povinen používat pro přidělení IP adresy nastavení automatického přiřazení. Nastavení statické IP adresy smí uživatel provést pouze po schválení Správcem sítě.
- 7.2. Koncové zařízení připojované do počítačové sítě VŠZ musí být odpovídajícím způsobem zabezpečeno vhodnou konfigurací systému, aplikací bezpečnostních záplat atd. V případě nedostatečně zabezpečeného nebo zavirovaného koncového zařízení může Správce sítě dočasně odejmout právo přístupu do počítačové sítě VŠZ a uživatel plně zodpovídá za škody způsobené porušením tohoto bodu.
- 7.3. V bezdrátové síti VŠZ je zakázáno provozovat serverové aplikace.
- 7.4. Veškeré bezdrátové přístupové body musí mít zabezpečeno připojování uživatelů pomocí uživatelského jména a hesla. Jiná poskytovaná připojení jsou v rozporu s tímto vnitřním předpisem.

Článek 8.

Elektronická pošta

- 8.1. Elektronická pošta slouží pro výměnu krátkých sdělení a dokumentů formou elektronických zpráv.
- 8.2. Pro používání elektronické pošty platí stejná pravidla jako pro používání běžné pošty dopravované provozovatelem poštovních služeb nebo přepravované jinou dopravní službou, zejména z hlediska listovního tajemství.
- 8.3. Velikost přenášených zpráv elektronické pošty může být omezena. Konkrétní limit je dán technickými možnostmi VŠZ.
- 8.4. Kapacita elektronické poštovní schránky uživatele je omezena, omezení je dáno technickými možnostmi VŠZ. Při překročení uživatelského limitu využívaného diskového prostoru může dojít k automatickému zablokování dalšího příjmu elektronické pošty pro daného uživatele.
- 8.5. Uživatel je povinen dbát na to, aby jeho zprávy byly přesně adresované a označené výstižným předmětem. Dále je vyžadováno rozlišování přímých příjemců a příjemců v kopii, aby nedocházelo k nežádoucímu obtěžování ostatních uživatelů rozesíláním zbytečných hromadných zpráv.
- 8.6. Elektronická pošta patří mezi služby, které vyžadují identitu uživatele. Uživatel je povinen při odesílání zpráv elektronické pošty používat ze strany VŠZ přidělenou adresu elektronické pošty. Za přidělování jmen a přístupu ke službě odpovídá příslušný správce. Je zakázáno odesílání dopisů s falešnou identitou a anonymní přístup k elektronické poště.

- 8.7. Uživatel je povinen vyzvedávat si pravidelně doručenou poštu z přidělené adresy elektronické pošty.
- 8.8. Transport elektronické pošty zajišťují pouze oficiální poštovní servery počítačové sítě VŠZ schválené Správcem sítě. Přenos prostřednictvím jiných než oficiálních serverů a příjem elektronické pošty ze serverů, které nejsou ve správě Správce sítě, může vést k zablokování koncového zařízení i uživatele.
- 8.9. Za provozování elektronické pošty jednotlivých součástí VŠZ odpovídá Správce sítě.
- 8.10. O právech rozesílat hromadnou poštu přes speciální poštovní servery na danou součást VŠZ rozhoduje ředitel VŠZ.

Článek 9.

Sankce za nedodržení pravidel užívání počítačové sítě VŠZ a provozování programového vybavení

- 9.1. Poruší-li uživatel pravidla užívání počítačové sítě VŠZ a provozování programového vybavení VŠZ ve smyslu tohoto vnitřního předpisu způsobem, který brání bezproblémovému provozu počítačové sítě VŠZ nebo ve využívání síťových služeb ostatním uživatelům, ztrácí dnem zjištění porušení pravidel oprávnění užívat služeb počítačové sítě VŠZ, a to do dne, než prokazatelně zajistí nápravu a získá souhlas Správce sítě k opětovnému připojení.
- 9.2. Porušení pravidel jakýchkoliv povinností stanovených tímto vnitřním předpisem ze strany studenta VŠZ může být považováno za disciplinární přestupek ve smyslu příslušných ustanovení zákona o vysokých školách (§ 64 až 67). V takovém případě zaměstnanec nebo správce, který se o této skutečnosti doví, informuje o nastalé situaci bez zbytečného odkladu rektora nebo ředitele VŠZ. Rektor VŠZ rozhodne o sankci za disciplinární přestupek na základě návrhu disciplinární komise.
- 9.3. Porušení pravidel užívání počítačové sítě VŠZ ve smyslu tohoto vnitřního předpisu zaměstnancem VŠZ se považuje za porušení pracovních povinností ve smyslu příslušných ustanovení zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů. Každý, kdo zjistí porušení tohoto vnitřního předpisu, informuje svého příslušného správce. Zaměstnanec nebo správce je povinen informovat elektronickou poštou nebo osobně o nastalé situaci bez zbytečného odkladu vedoucího zaměstnance uživatele sítě (porušitele povinnosti). Vedoucí zaměstnanec následně postupuje v souladu se zákoníkem práce.

Ing. František Kunc, PhD., v. r.
ředitel

V Praze dne 1. 1. 2015