Smernica č. 2/2022

o manažmente informačných technológií v podmienkach Slovenskej zdravotníckej univerzity

(nákup, prideľovanie, podmienky využívania, vyraďovanie, bezpečnosť, ochrana dát a i.)

V súlade s príslušnými zákonmi o hospodárení štátnej inštitúcie predovšetkým Zákon 523/2004 Z. z. Zákon o rozpočtových pravidlách verejnej správy) sa požaduje, aby inštitúcia vykonávala svoju činnosť hospodárne a aby dbala na efektívne využívanie finančných prostriedkov. Z tohto dôvodu existujú aj práva inštitúcie vo vzťahu k zamestnancom v oblasti správy majetku IT.

Smernica upravuje pravidlá v oblasti správy a využívania informačných technológií (HW + SW) a správy a využívania samotnej informačnej techniky (HW), ktorá je prideľovaná k výkonu pracovných činností zamestnancov SZU tak, aby vytvárali predpoklad pre optimálne podmienky pre ich pedagogickú, vedecko-výskumnú a administratívnu činnosť. Smernica slúži tiež na to, aby zamestnanec poznal rozsah svojich možných požiadaviek vo vzťahu k vybaveniu IT technikou pre svoje pracovné činnosti.

Smernica nerieši konkrétne postupy, ktoré už riešia Zákony, resp. interné normy SZU (napr. spôsob obstarávania IT techniky vo vzťahu k dodávateľom a p.). Je rozdelená na dve časti:

I. Informačná technika – pracovná pomôcka zamestnanca SZU
II. Zásady ochrany, servisu a bezpečnosti dát pri využívaní informačných technológií

Smernica IT je vypracovaná v súlade so zákonom č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Smernica IT platí pre všetkých zamestnancov SZU používajúcich informačné technológie SZU.

ČASŤ I.

Informačná technika – pracovná pomôcka zamestnanca SZU

1. Úloha smernice a základné vymedzenie

1.1. Význam skratiek

IT	Informačné technológie
ITCH	Informačná technika
IS	Informačné systémy
HW	Hardware
PPC	Pevná počítačová stanica
LAN	Lokálna počítačová sieť
NTB	Notebook
MO	Monitor
PTL	Personálna tlačiareň
STL	Sieťová tlačiareň

SL	Slúchadlá
PRP	Prídavné reproduktory
PCAM	Prídavná kamera
KL	Klávesnica
M	Myš
SCAN	Skener
EXD	Externý disk
USBK	USB kľúč
TV	Televízor
TBL	Tablet

1.2. Úlohou smernice v Časti I. je určenie všeobecných pravidiel pre pridelenie ITCH zamestnancovi, pravidiel a zodpovednosti pri jej využívaní, pri jej evidencii a presunoch, pri zmene užívateľa a p..

1.3. Nárok na ITCH, jej rozsah a technické parametre neurčuje zamestnanec SZU, ale vyplývajú z jeho pracovného zaradenia, z nutnosti využívať ITCH a z technických štandardov SZU, ktoré sú priebežne aktualizované. Štandardy nemusia byť porovnateľné so štandardami iných organizácií. Ich kvalitatívne parametre závisia od objemu disponibilných finančných prostriedkov na nákup ITCH a nutnosti obmeny tej techniky, ktorá je už nevyhovujúca. Limituje ju aj priemerná technická úroveň všetkých zariadení využívaných zamestnancami SZU.

1.4. ITCH môžu zamestnanci využívať výlučne pre pracovné účely. SZU disponuje technickými prostriedkami, ktoré dokážu v prípade potreby prehliadať aktivity na jednotlivých ITCH, ktoré majú priradené IP adresy (PPC, notebook, STL). Zamestnávateľ ich má právo kontrolovať v súlade s príslušnými zákonmi a pri zabezpečení ochrany osobných údajov (§ 13 ods. 4 zákona č. 311/2001 Z. z., zákonník práce, § 13 odst. 7 zákona č. 311/2001 Z. z., zákonník práce, Zákon č. 18/20218 Z.z. o ochrane osobných údajov). Takúto možnosť SZU využije len a výlučne v súvislosti s hospodárnym využívaním ITCH a využívaním fondu pracovnej doby.

1.5. Zamestnanec, ktorému bola zverená ITCH je povinný starať sa o jej využívanie v súlade s bežnými technickými štandardami, dbať o jej funkčnosť, zabrániť jej poškodeniu a znehodnoteniu.

1.6. Zamestnanec zodpovedá za nedbalostné a úmyselné škody na jemu zverenej ITCH a to do výšky, o ktorej rozhodne Škodová komisia SZU.

2. Nárok zamestnanca na ITCH

2.1. Na pridelenie ITCH má nárok zamestnanec zaradený v pracovnom pomere na základe riadnej pracovnej zmluvy, s úväzkom vyšším ako 0,6. Zamestnanci vykonávajúci prácu na základe dohôd, resp. úväzku nižšieho ako 0,6 nemajú nárok na pridelenie ITCH, s výnimkou tých zamestnancov, ktorí majú odôvodnený nárok dôvodmi, ktoré sú špecifikované v iných bodoch Smernice.

2.2. V osobitných prípadoch , predovšetkým v súvislosti s prácou na klinikách SZU, môže dekan príslušnej fakulty navrhnúť vybavenie zamestnanca ITCH aj v prípade, že jeho úväzok je nižší ako 0,6. V závislosti na finančných možnostiach takýto návrh schvaľuje kvestor SZU. Rovnaký postup platí aj pre pridelenie PPC na katedrách a pracoviskách, kde nie je ani u jedného zamestnanca dosiahnutý úväzok 0,6, avšak pracovisko musí byť vybavené PPC.

2.3. Požiadavku na vybavenie zamestnanca ITCH predkladá v súlade s inými pravidlami (nariadenie kvestora o obstarávaní..) tajomníčka fakulty, resp. riaditeľ rektorátneho útvaru, ktorí majú zároveň v zmysle spomenutého nariadenia prístup do systému SOFTIP Approval.

2.4. Zamestnanec definovaný v zmysle bodu 2.1. má nárok na pridelenie len jedného ITCH (NTB alebo PPC + zodpovedajúce prídavné periférne zariadenia). Zamestnancovi bude pri pridelení ITCH prednostne ponúknuté využívanie NTB a to vzhľadom k tomu, že súčasná organizácia práce a rovnako aj organizácia práce v budúcnosti predpokladá vyššiu flexibilitu zamestnanca, pokiaľ ide o miesto výkonu jeho práce (HO).

2.5. Vo výnimočných prípadoch na základe odporúčania dekana fakulty, kvestora, alebo riaditeľov rektorátnych útvarov, môže mať zamestnanec pridelenú aj ďalšiu ITCH (PPC, NTB). O schválení rozhodne kvestor v závislosti na aktuálnych finančných možnostiach univerzity.

2.6. Druhá, prípadne ďalšia ITCH (PPC, NTB), ktorú k dátumu účinnosti tejto Smernice využíva jeden zamestnanec, bude zamestnancovi odobratá a pridelená tým zamestnancom, ktorých ITCH je pod súčasným bežným štandardom a ktorí nemôžu využívať nutné nástroje IT dostupné na SZU. Tento proces bude zabezpečovaný postupne. Zamestnancovi bude k dispozícii 14 dňová lehota na presun dát do ITCH, ktoré si chce ponechať. V prípade, že bude zamestnanec požadovať NTB ako náhradu za viaceré PPC, ktoré v súčasnosti využíva, v rámci možnosti mu bude vyhovené.

2.7. Ambulancie SZU majú nárok na PPC umiestnenú v ambulancii, pričom sa na pridelenie PPC nevzťahuje bod 2.1. a 2.4..

2.8. Zariadenia využívané ad hoc. (audio súpravy, mikrofóny, záznamové zariadenia a pod.) môžu byť pridelené priamo ku konkrétnemu ITCH, alebo ich umiestnenie v danom čase sa bude riadiť podľa požiadaviek tajomníčka fakulty, keďže každá fakulta disponuje dostatočným množstvom týchto zariadení.

3. **Zodpovednosť za zverený majetok ITCH**

3.1. ITCH, rovnako ako ostatný majetok univerzity daná do užívania zamestnancovi, musí byť riadne a presne evidovaná na karte zamestnanca. Po vecnej stránke a po stránke pravdivosti a zhody údajov so skutočným stavom zodpovedá tajomníčka fakulty, resp. riaditeľ rektorátneho útvaru.

3.2. Tajomníčka fakulty a riaditelia rektorátnych útvarov zodpovedajú za to, že takto pridelená ITCH je následne evidovaná na karte zvereného majetku konkrétneho zamestnanca. Taktiež zodpovedajú za vysporiadanie zvereného majetku v prípade odchodu zamestnanca zo zamestnania, resp. jeho presunu na iné pracovisko SZU.

3.3. ITCH umiestnená v učebniach je evidovaná na karte zverených ITCH tajomníčky fakulty, ktorá zodpovedá za jej správne a účelné využívanie. Táto technika sa za žiadnych okolností nesmie presúvať k zamestnancovi bez riadne zdôvodneného a IT oddelením schváleného súhlasu.

3.4. ITCH prislúchajúca k laboratóriám, resp. iným špecifickým pracoviskám je evidovaná na karte zverených ITCH vedúceho daného strediska. Táto technika sa za žiadnych okolností nesmie presúvať k zamestnancovi bez riadne zdôvodneného a IT oddelením schváleného súhlasu.

3.5. Za škody, ktoré SZU vzniknú nedodržaním tohto postupu zodpovedá tajomníčka fakulty, resp. riaditeľ rektorátneho útvaru.

3.6. Tajomníčka fakulty, resp. riaditeľ rektorátneho útvaru taktiež zodpovedá za vedenie inventárneho zoznamu ITCH zamestnancov danej fakulty, resp. útvaru, s povinnosťou k určenému dátumu (dátum inventarizácie vyhlásený kvestorom) predložiť oddeleniu správy majetku zoznam ITCH a ich užívateľov, resp. zabezpečiť rýchly a hladký priebeh fyzickej inventarizácie.

3.7. Svojvoľné presúvanie ITCH medzi zamestnancami bez súčasného záznamu v inventarizácii je neprípustné. O prípadný presun je potrebné požiadať oddelenie IT, ktoré najprv vykoná technickú prehliadku ITCH a následne vydá

súhlas na presun. Tajomníčka fakulty, resp, riaditeľ rektorátneho útvaru tento presun zaeviduje následne na kartách zvereného majetku odovzdávajúceho ITCH a jeho prijímateľa.

3.8. ITCH určené pre zabezpečenie, resp. podporu celouniverzitných procesov (servery, prístroje na monitorovanie, STL a p.) spadajú do správy odd. IT a podliehajú osobitnej evidencii.

4. Zdroje financovania ITCH

4.1 Manažovaniu IT v zmysle tejto smernice podlieha ITCH zakúpená z finančných prostriedkov hlavnej činnosti, podnikateľskej činnosti a NRC. V prípade nákupu ITCH z finančných prostriedkov projektov, zodpovedá za účelné umiestnenie ITCH vedúci konkrétneho projektu. V prípade nákupu ITCH z darovaných finančných prostriedkov bude univerzita zohľadňovať tieto súvislosti:

a) ak darované finančné prostriedky boli poskytnuté priamo na meno konkrétneho zamestnanca – v takomto prípade bude rešpektovaný pokyn darcu
b) ak darované finančné prostriedky boli poskytnuté pracovisku, resp. univerzite – v takom prípade dar podlieha pravidlám, ktoré platia pre nákupy ITCH z prostriedkov SZU

5. Správa ITCH v prevádzke

5.1. Návrh na vyradenie ITCH predkladá tajomníčka fakulty, resp. riaditeľ rektorátneho útvaru oddeleniu IT a to požiadavkou na adresu servis.it@szu.sk s uvedením čísla IN, pod ktorým je zariadenie evidované. Po preskúmaní stavu ITCH pracovníkom IT, bude rozhodnuté o jej vyradení, presune, resp. ponechaní v užívaní.

5.2. Technické parametre konkrétnej ITCH podliehajú štandardu, ktorý v aktuálnom období stanovuje oddelenie IT. Tento štandard sa vzťahuje na všetky technické parametre a nie je možné požadovať ITCH pre bežné využitie vo vyššom štandarde. Výnimku môže potvrdiť zodpovedný IT pracovník po konzultácii so žiadateľom a to v prípade, že ITCH bude využívaná pre nadštandardné programovanie, alebo spracovanie dát, predovšetkým s dátami laboratórií, vedeckých úloh a pod..

5.3. Ďalším spôsobom získania nadštandardného vybavenia IT je kúpa zariadenia zo sponzorských prostriedkov, v zmysle bodu 4.1. a) ak darované finančné prostriedky boli poskytnuté priamo na meno konkrétneho zamestnanca – v takomto prípade bude rešpektovaný pokyn darcu.

5.4. Vyradenie ITCH sa riadi príslušnými predpismi SZU pre vyraďovanie majetku a výlučne v spolupráci navrhovateľa na vyradenie ITCH, odb. IT a odb. EaF SZU.

5.5. Likvidáciu vyradeného majetku zabezpečuje odd. Prevádzky SZU v súlade s dodržaním platných zákonov o narábaní s odpadmi.

ČASŤ II.

Zásady ochrany, servisu a bezpečnosti dát pri využívaní informačných technológií

1. **Práva a povinnosti zamestnanca** (ďalej užívateľ)**, práva a povinnosti zodpovedného zamestnanca oddelenia IT** (ďalej informatik)

1.1. Všetci užívatelia sú povinní dodržiavať ustanovenia tejto smernice; zároveň je každý užívateľ IS SZU povinný dodržiavať všetky ustanovenia Zákona č. 18/20218 Z. z. o ochrane osobných údajov, najmä zachovávať mlčanlivosť o osobných údajoch v IS SZU.

1.2. Užívateľ pracuje výhradne na pridelenom PC pod svojim užívateľským menom a heslom. Je plne zodpovedný za škody, vzniknuté zneužitím jeho konta v dôsledku nedbalosti. Dáta uložené na pracovných staniciach a serveroch IS sú vo vlastníctve SZU a to aj v prípade, ak boli prenesené na dátové médiá.

1.3. Užívateľ je povinný si naštudovať interné manuály k IS SZU formou individuálneho štúdia, príp. absolvovať povinné plánované školenia, alebo ho zaškolí iný zamestnanec.

1.4. Užívateľ nepoužije žiadne prostriedky na získanie iných prístupových práv, či privilegovaného stavu, než ktorý mu bol pridelený informatikom, ani sa nepokúsi získať neoprávnený prístup k chráneným informáciám a údajom iných užívateľov. Užívateľ sa nesmie pokúšať o prienik do iných sieťových zdrojov a systémov, u ktorých nemá oprávnenie k prístupu.

1.5. V prípade, ak užívateľ zistí, že jeho reálne pridelené prístupové práva nezodpovedajú úrovni schválených prístupových práv, je povinný požiadať cez tajomníčku fakulty informatika, ktorý mu práva pridelil, o ich zmenu. Ten rozhodne, či žiadosti vyhovie.

1.6. Užívateľ je povinný v prípade opustenia pracoviska sa odhlásiť z PC (IS SZU) riadnym a korektným ukončením prostredia operačného systému (MS Windows) a všetkých spustených programov. Užívateľ je povinný pri odchode z pracoviska (na služobnú cestu, koniec pracovnej doby, práce neschopnosť a pod.) počítač korektným spôsobom vypnúť.

1.7. Užívateľ je povinný v prípade krátkodobého opustenia pracoviska (prípad, že sa v priebehu dňa vráti na pracovisko) uzamknúť PC.

1.8. Užívateľ je povinný dodržiavať nasledovné základné pravidlá obsluhy PC a jeho periférnych zariadení:

a) zapnutie zariadení vykonávať v poradí tlačiareň, monitor, základná jednotka personálneho počítača, vypínanie zariadení vykonávať v opačnom poradí až po korektnom ukončení všetkých programov,

b) pri výpadku elektrického napájania je nevyhnutné ihneď vypnúť sieťový vypínač personálneho počítača a všetkých periférnych zariadení, informovať sa o príčine výpadku a riešiť situáciu v spolupráci so zodpovednými zamestnancami SZU,

c) ak pri štarte, prevádzke PC, alebo periférneho zariadenia dôjde k chybovému stavu, ktoré je identifikované chybovým hlásením na monitore alebo zvukovým signálom, okamžite prerušiť prácu, nereštartovať PC a informovať informatika,

d) užívateľ neprerušuje proces bootovania personálneho počítača stláčaním akýchkoľvek kláves,

e) užívateľ môže vypnúť personálny počítač len po korektnom ukončení činností všetkých aplikačných programov (MS Word, MS Excel a pod.).

1.9. Užívateľ je povinný používať osobný počítač a periférne zariadenia tak, aby nedošlo k ich mechanickému poškodeniu, znečisteniu a je povinný ich udržiavať v čistom stave.

1.10. Z hľadiska ochrany údajov nachádzajúcich sa na lokálnych pamäťových médiách personálnych počítačov, na pamäťových médiách centrálnych výpočtových kapacít IS SZU, alebo pri práci s prenosnými pamäťovými médiami je najväčším nebezpečenstvom infiltrácia počítačovým vírusom, alebo neoprávneným zásahom nepovolanej osoby. Z týchto dôvodov je užívateľ povinný dodržiavať základné zásady ochrany pevného disku personálneho počítača pred napadnutím počítačovými vírusmi a zásady ochrany a používania hesiel.

1.11. Základné zásady ochrany pevného disku personálneho počítača pred napadnutím počítačovými vírusmi:

a) skontrolovať každé pripájané prenosné pamäťové médium k PC inštalovaným antivírusovým programovým vybavením,

b) pred spustením operačného systému personálneho počítača odpojiť všetky externé pamäťové média (USB disky a pod.),

c) sledovať hlásenia antivírusového programového vybavenia,

d) pri zistení prítomnosti počítačového vírusu v súboroch, alebo správach v elektronickej pošte a neúspešnom odstránení antivírusovým programovým vybavením, alebo pri podozrení na jeho výskyt, okamžite

prerušiť akúkoľvek činnosť s personálnym počítačom a túto skutočnosť bezodkladne osobne, alebo telefonicky nahlásiť informatikovi.
V žiadnom prípade užívateľ nesmie takto napadnutý súbor, alebo správu posielať ďalej mailom inému užívateľovi, alebo informatikovi,

e) Užívateľ nesmie nikdy odpovedať na maily, v ktorých sa vyskytuje požiadavka na poskytnutie prístupových údajov užívateľa, osobných údajov a podobne.

1.12. Užívateľ je povinný na personálnom počítači používať výlučne programové vybavenie, ktoré je nainštalované informatikom.

1.13. V prípade, ak užívateľ zistí, že došlo k porušeniu ustanovení tejto smernice, je povinný túto skutočnosť ohlásiť príslušnému vedúcemu útvaru a následne informatikovi.

1.14. Užívateľ je povinný umožniť prístup informatikovi do jeho personálneho počítača. Informatik je povinný oznámiť užívateľovi dôvod zásahu.

1.15. Užívateľovi je zakázané:

a) bez predchádzajúceho súhlasu informatika, alebo priameho nadriadeného sa prihlasovať do LAN a IS SZU z iného personálneho počítača než z toho, ktorý mu bol pridelený,

b) umožniť používať jemu pridelený personálny počítač neoprávneným osobám, pričom neoprávnenou osobou v tejto súvislosti je osoba, ktorá nie je užívateľom,

c) prihlasovať sa do LAN a IS SZU pod cudzím menom,

d) pripájať akékoľvek nové personálne počítače do LAN SZU bez vedomia informatika,

e) inštalovať na počítač softvér, na ktorý SZU nemá platnú licenciu, alebo súhlas autora,

f) meniť alebo mazať akékoľvek súbory, ktoré neboli ním vytvorené, s dôrazom na systémové alebo konfiguračné súbory inštalovaného programového vybavenia operačného systému,

g) kopírovať existujúce programové vybavenie z lokálnych pamäťových médií personálnych počítačov a pamäťových médií centrálnych výpočtových kapacít LAN a IS SZU na iné pamäťové médium,

h) akýmkoľvek spôsobom zneužiť programové vybavenie z lokálnych pamäťových médií centrálnych výpočtových kapacít LAN a IS SZU a toto sprístupniť inej osobe,

i) vynášať údaje na prenosných pamäťových médiách mimo SZU okrem prípadov, ktoré povolí vedúci príslušného útvaru SZU, alebo okrem prípadov, ktoré sú upravené v zmluvách SZU s inými právnymi subjektmi,

j) vyvíjať činnosť smerujúcu k prelomeniu bezpečnostných bariér LAN a IS SZU,

k) vykonávať akékoľvek presuny personálnych počítačov a periférnych zariadení bez vedomia príslušného vedúceho útvaru, informatika a pracovníka zodpovedného za evidenciu majetku, zamestnanec musí pri presune zariadení zabezpečiť prítomnosť informatika,

l) akýmkoľvek spôsobom zasahovať do konfigurácie BIOS-u personálneho počítača,

m) pripájať a používať súkromné PC a zariadenia do LAN SZU.

1.15. Všetky dokumenty ukladané na pevnom disku pracovnej stanice je doporučené zálohovať prideleným úložiskom v cloude. Za stratu dôležitých dokumentov v prípade havárie pracovnej stanice je zodpovedný užívateľ.

1.16. Užívateľ prenosného počítača je povinný navyše:

a) zabezpečiť ochranu prenosného počítača pred odcudzením, prípadne poškodením, zavírením,

b) nepripájať sa do verejných počítačových sietí bez zabezpečenia dostatočnej ochrany údajovej základne nachádzajúcej sa na prenosnom počítači.

1.17. Užívateľ nesmie pripojiť žiadne zariadenia k pracovnej stanici zapojenej do počítačovej siete. V prípade zistenia pripojenia uvedených zariadení je informatik povinný zablokovať prístup užívateľa do IS a zabezpečiť odpojenie zariadení.

1.18. Užívateľ môže využívať externé dátové médiá výlučne na plnenie svojich služobných/pracovných povinnosti.

1.19. Užívateľ má právo využívať všetky technické a programové prostriedky a služby LAN a IS SZU v rozsahu jemu pridelených prístupových práv informatikom.

1.20. Prístupové práva užívateľa a pridelené programové vybavenie sú odvodené od jeho funkčného zaradenia v organizácii a jeho pracovnej náplne. Užívateľ má právo požiadať prostredníctvom svojho priameho nadriadeného pridelenie vyšších prístupových práv, ak práva ktoré mu boli pridelené, nie sú postačujúce pre vykonávanie špecifického druhu činnosti, alebo pre sprístupnenie konkrétneho druhu informácií.

1.21. Užívateľ má právo požiadať informatika, alebo osobu na to určenú o poskytnutie technickej podpory pri riešení problémov spojených

s prevádzkou programového a technického vybavenia LAN a IS SZU.

1.22. Užívateľ má právo navrhovať zavedenie, inštalovanie nového aplikačného programového vybavenia a dávať podnety na vylepšenie existujúceho a dať návrh na zabezpečenie nového APV (ktoré v rámci SZU nie je pokryté).

1.23. Užívateľ má právo navrhovať rozšírenie poskytovaných služieb IS SZU a aktívne sa podieľať pri ich zavádzaní.

1.24. Užívateľ má právo poskytovať námety smerujúce k skvalitneniu a zefektívneniu práce IS SZU.

1.25. Informatici sú v rozsahu svojich práv a povinností vymedzených pracovnou náplňou a touto smernicou zodpovední za prevádzku LAN SZU, IS SZU a za prevádzku, inštaláciu a aktualizáciu APV.

1.26. Informatici sú oprávnení:

a. konfigurovať a vykonávať zmeny v konfigurácii všetkých personálnych počítačov, periférnych a komunikačných zariadení zapojených v LAN SZU,

b. pripájať personálne počítače, komunikačné a periférne zariadenia do LAN SZU,

c. v odôvodnených prípadoch odpojiť personálny počítač užívateľa z LAN SZU,

d. v odôvodnených prípadoch rozhodnúť o umiestnení technických zariadení LAN SZU v budove SZU,

e. vykonávať kontrolu personálnych počítačov užívateľov LAN a IS SZU,

f. meniť konfiguráciu LAN SZU, resp. prideľovať a meniť prístupové práva užívateľom LAN a IS SZU,

g. rozhodovať o spôsobe integrácie technických zariadení a programového vybavenia do LAN a IS SZU,

h. prideľovať priestor na pamäťových médiách centrálnych výpočtových kapacít LAN SZU a v odôvodnených prípadoch meniť veľkosť tohto priestoru,

i. spolurozhodovať o nasadení nových technických zariadení do LAN a IS SZU.

1.27. Informatici nie sú oprávnení vlastniť, konfigurovať a spravovať užívateľské konto (meno/heslo) do informačných systémov, v ktorých sú vedené osobné a mzdové údaje zamestnancov SZU.

1.28. Informatici nie sú oprávnení vstupovať do užívateľského konta, ktoré je zabezpečené heslom. V špecifických prípadoch je potrebný prístup informatika do užívateľského konta, ktoré je chránené heslom s podmienkou, že prístupové heslo zadá sám užívateľ.

1.29. Informatici sú povinní:

a. optimalizovať prevádzku LAN a IS SZU,

b. pravidelne vytvárať záložné kópie aplikačného programového vybavenia a dátového fondu nachádzajúceho sa na serveroch LAN a IS SZU,

c. vykonávať správu užívateľských prístupových hesiel,

d. zablokovať konto užívateľa, ak je odôvodnené podozrenie z jeho zneužitia,

e. viesť evidenciu o užívateľoch LAN a IS SZU a ich prístupových právach k aplikáciám,

f. chrániť servery LAN a IS SZU heslom,

g. v rozsahu svojich právomocí zabrániť porušovaniu tejto smernice,

h. priebežne kontrolovať dodržiavanie tejto smernice,

i. písomne informovať priameho nadriadeného užívateľa o závažnom, alebo opakovanom porušení tejto smernice,

j. riešiť v súčinnosti s vedením každé porušenie tejto smernice,

k. poskytovať pomoc a podporu užívateľom LAN a IS SZU,

l. zachovávať mlčanlivosť o konfigurácii LAN a IS SZU v zmysle zákona, Zákon č. 18/20218 Z.z. o ochrane osobných údajov

m. bezodkladne ohlásiť vedúcemu OIT havarijný a servisný stav,

n. pri odstraňovaní poruchy byť osobne účastný,

o. inštalovať nové aktualizácie systémového a aplikačného programového vybavenia SZU.

1.30. Práva a povinnosti informatika pri mimoriadnych situáciách, za ktoré sa z hľadiska prevádzky IS SZU považuje:

a. neoprávnené oboznámenie sa s prístupovým heslom správcu LAN a IS SZU,

b. neautorizovaný prístup do LAN a IS SZU,

c. pokus o neautorizovaný prístup do LAN SZU,

d. nestabilný chod systémového a aplikačného programového vybavenia,

e. narušenie fyzickej bezpečnosti LAN a IS SZU,

f. prítomnosť a pôsobenie počítačového vírusu,

g. výpadok elektrického napájania LAN SZU dlhší ako 10 minút,

h. požiar, výbuch alebo iný druh havárie,

i. živelná pohroma a katastrofa,

j. hrozba teroristického útoku,

k. teroristický útok,

l. vyhlásenie vojnového stavu,

m. každé porušenie tejto smernice.

1.31 Informatici majú právo v prípade mimoriadnych udalostí vymenovaných v časti II v bode 1.30 tejto smernice okamžite, bez akejkoľvek výstrahy, zastaviť činnosť LAN SZU, alebo ktoréhokoľvek jej logického celku, príp. zariadenia.

1.32 Informatici sú v prípade mimoriadnych udalostí vymenovaných v časti II v bode 1.30 tejto smernice povinní postupovať tak, aby svojou činnosťou zamedzili vzniku škody, prípadne minimalizovali rozsah škôd, spôsobených touto udalosťou na dátovom fonde, technickom a programovom vybavení SZU.

1.33. Informatici sú povinní bezodkladne informovať o situácii vedúceho OIT, ktorý rozhodne o ďalšom postupe.

1.34. Informatici sú oprávnení vytvoriť užívateľské konto, prípadne umožniť pracovať s technickými a programovými prostriedkami IS SZU novým zamestnancom iba na základe písomnej žiadosti Personálno-právneho odboru SZU (v zmysle smernice 8/2016).

2. Zásady používania hesiel

2.1. Základné zásady používania hesiel a ich ochrany pred zneužitím nepovolanými osobami:

a) periodicky, najmenej jeden krát za 90 dní zmeniť používané heslo na pridelenom PC,

b) pamätať si heslo bez jeho zaznamenania na iných médiách (papier, USB kľúč a pod.),

c) udržiavať mlčanlivosť o všetkých heslách,

d) pri zistení alebo podozrení, že došlo k neoprávnenému oboznámeniu sa s ktorýmkoľvek z jemu pridelených hesiel, okamžite zmeniť heslo

a informovať písomne priameho nadriadeného a informatika o tomto bezpečnostnom incidente.

e) V prípade, že si užívateľ zmeniť heslo nemôže, musí požiadať o nové heslo informatika.

2.2 Užívateľ je povinný dodržiavať nasledujúce zásady tvorby hesla:

a) heslo musí mať dĺžku minimálne 8 znakov,

b) heslo musí obsahovať minimálne 1 znak z každej kategórie:

- veľké písmená (A - Z),
- malé písmená (a – z),
- čísla z desiatkovej sústavy (0 – 9),

c) meno a heslo nesmie byť zhodné,

d) meno a heslo nesmie obsahovať diakritiku

e) odporúča sa, aby :

- heslo nebolo menom ani názvom,
- heslo nebolo odvodené od personálií užívateľa,
- heslo nebolo tvorené priamou postupnosťou kláves na klávesnici,
- každé použité heslo bolo jedinečné,
- pri zmene hesla sa nové heslo od pôvodného líšilo najmenej v štyroch znakoch

3. Zásady používania počítačovej siete SZU, Internetu

3.1. Užívateľ berie na vedomie, že poverená osoba zamestnávateľa má prístup k metadátam akejkoľvek činnosti užívateľa s IT. Preto je zamestnávateľ oprávnený zisťovať rozsah a spôsob využitia IT a siete.

3.2. Prístup k sieti Internet nie je dovolené používať na súkromné účely.

3.3. Je zakázané používať akýkoľvek komunikačný prostriedok využívajúci Internet (napr. Facebook, WhatsApp, Viber, Skype a pod.) na súkromné účely. Túto činnosť je možné využívať len pre dištančné vzdelávanie a služobnú komunikáciu, pre ktorú sa odporúča prednostne využívať MS Teams.

3.4. Je zakázané používať LAN SZU k neoprávnenému prístupu do iných sietí, k šíreniu počítačových vírusov a iných škodiacich alebo činnosť sledujúcich programov, či skriptov (spyware, malware, ap.).

4. Opravy a údržba technických zariadení a programového vybavenia IS SZU

4.1 Opravy a údržbu technických zariadení IS SZU zabezpečuje výlučne OIT na základe požiadavky mailom na adresu servis.it@szu.sk, alebo telefonicky vedúcemu OIT, ktorý toto následne pridelí informatikovi ako úlohu. Evidenciu a prideľovanie úloh zabezpečuje vedúci OIT

4.2 V prípade, že informatik zistí na personálnom počítači užívateľa prítomnosť počítačového vírusu, vykoná všetky opatrenia na zabránenie jeho ďalšiemu šíreniu.

4.3 Informatik je oprávnený v prípade nutnosti odpojiť personálny počítač z LAN SZU.

4.4 V prípade, že je za účelom opravy personálneho počítača nevyhnutné, aby bol vynesený mimo budovu SZU, užívateľ prideleného personálneho počítača je povinný zabrániť úniku citlivých údajov mimo SZU.

5. Zásady bezpečnosti LAN a IS SZU

5.1. Fyzická ochrana serverovní

a. Serverovne sú umiestnené v priestoroch SZU v uzamykateľných miestnostiach.

b. Kľúče od zámkov dverí serverovní sú vyhotovené v potrebnom počte kópií ku každým dverám, z ktorých jedna kópia je umiestnená na OIT.

c. Do serverovní sú oprávnení vstupovať výlučne informatici, alebo ich nadriadení.

d. Centrálne výpočtové kapacity a komunikačné zariadenia LAN a IS SZU musia byť, pokiaľ to technické riešenie umožňuje, elektricky napájané zo zálohového zdroja.

5.2. Vstup pracovníkov inej organizácie, ktorí vykonávajú v rámci svojej činnosti údržbu a servis koncových zariadení, je za predpokladu, že majú podpísané čestné prehlásenie o zachovaní mlčanlivosti. Tretie strany môžu vykonávať práce v serverovej miestnosti len za prítomnosti informatika.

6. Práca cudzích osôb v LAN a IS SZU

6.1. Cudzou osobou sa v tejto smernici rozumie osoba, ktorá nie je zamestnancom SZU.

6.2. Cudzia osoba môže pracovať v LAN a IS SZU výlučne na základe písomného súhlasu vedúceho príslušného útvaru, pre ktorý sa práca vykonáva a ktorý je povinný informovať vedúceho OIT.

6.3. Písomný súhlas sa vydáva na konkrétnu činnosť a konkrétne časovo obmedzené obdobie.

6.4. Písomný súhlas musí obsahovať:

a. meno, priezvisko, príp. tituly cudzej osoby,

b. názov organizácie, v mene ktorej je činnosť vykonávaná,

c. presný dátum, kedy možno činnosť vykonávať,

d. stručný popis vykonávanej činnosti,

e. dátum vydania a podpis vedúceho príslušného útvaru.

6.5. Cudzia osoba vykonáva činnosť výlučne za prítomnosti užívateľa IS SZU.

7. ZÁVEREČNÉ USTANOVENIA

7.1. Každý zamestnanec SZU je povinný prostredníctvom vedúceho útvaru, upozorniť na nedostatky vo vydanom dokumente a môže vznášať návrhy na zmeny.

7.2. Kontrolou plnenia zásad a dodržiavania tejto smernice sú poverení:

a. vedúci jednotlivých útvarov SZU

b. hlavný kontrolór SZU

7.3. Kontrolou aktuálnosti tejto smernice je poverený vedúci OIT .

7.4. Táto smernica nadobúda účinnosť dňom jej podpisu rektorom SZU.

V Bratislave dňa 23. 6. 2022

Dr. h. c. prof. MUDr. Peter Šimko, CSc., v. r.

rektor SZU