IT SMERNICA O KYBERNETICKEJ BEZPEČNOSTI

FAKULTNEJ NEMOCNICE S POLIKLINIKOU NOVÉ ZÁMKY

Schválil: MUDr. Jozef JEŽÍK		generálny riaditeľ		**Dátum:**	**Podpis:**
Schválil: Ing. Ľubica BARTOŠOVÁ		ekonomická riaditeľka		**Dátum:**	**Podpis:**
Schválil: MUDr. Zoltán DANCZI		medicínsky riaditeľ		**Dátum:**	**Podpis:**
Preskúmal/posúdil: Ing. Ladislav ČERI		Manažér kvality		**Dátum:**	**Podpis:**
Vypracoval: Ing. Ladislav SLOBODA		vedúci Odboru informatiky		**Dátum:**	**Podpis:**
Výtlačok číslo:		**Platnosť od:**	dátumu schválenia	**Účinnosť od:**	**15.07.2019**
Úsek:	ER	**Verzia/ počet strán:**	V1-1/31	**Reg. značka:**	**C.1.6**
Odbor/oddelenie:	OINF	**zo dňa:**	15.07.2019	**Znak hodnoty a lehota uloženia:**	A-2 (po strate platnosti)
Ruší sa platnosť dokumentu: IT smernica – verzia 0.					

OBSAH

ZOZNAM SKRATIEK A POJMOV

FNsP – prevádzkovateľ - Fakultná nemocnica s poliklinikou Nové Zámky, Slovenská 2323/11 A, 94034 Nové Zámky

OINF – odbor informatiky

IT – informačné technológie

Zákon – Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti (ZoKB)

Vyhláška – Vyhláška NBÚ č. 362/2018

Úrad – Národný bezpečnostný úrad SR

GDPR - Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

Základná služba – služba, ktorá je zaradená v zozname základných služieb a

1. závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore ZoKB
2. je informačným systémom verejnej správy, alebo
3. je prvkom kritickej infraštruktúry

Prevádzkovateľ základnej služby – orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu službu podľa predošlého bodu.

Sprostredkovateľ podľa 18/2018 Z.z. je každý, kto spracúva osobné údaje v mene prevádzkovateľa, v rozsahu a za podmienok dojednaných s prevádzkovateľom v písomnej zmluve podľa § 8 a v súlade so zákonom o ochrane osobných údajov.

Aktívum – subjekt, ktorý má určitú hodnotu a je potrebné ho chrániť. Aktíva informačného systému sú softvér, hardvér, údaje, komunikačné prostriedky a zamestnanci, ktorých organizácia používa na zabezpečenie informatických služieb.

Vlastník aktíva – je organizačný útvar FNsP Nové Zámky, ktorý špecifikuje funkčné vlastnosti aktíva, zodpovedá za jeho funkčnosť a ochranu a autorizuje prístupové práva používateľov k aktívu. K základným aktívam spoločnosti patria moduly IS a príslušné údaje a technické prostriedky.

Analýza rizík – preskúmanie vzťahov medzi aktívami, hrozbami, bezpečnostnými slabinami a opatreniami s cieľom určiť aktuálnu úroveň rizík.

Bezpečnostná brána (Firewall) – je zariadenie, ktoré realizuje bezpečné oddelenie chránenej vnútornej (privátnej) počítačovej siete od inej počítačovej siete alebo nechránenej (verejnej) siete, napríklad Internetu. Existuje viacero konfigurácií bezpečnostných brán.

Bezpečnostná slabina – stav zraniteľnosti zapríčinený nedostatkom bezpečnostného opatrenia alebo jeho neprítomnosťou.

Bezpečnostné opatrenie – ľubovoľné zariadenie alebo akcia resp. predpis so schopnosťou/cieľom redukovania bezpečnostných slabín a hrozieb.

Bezpečnostný incident – je akákoľvek aktivita používateľa alebo iného subjektu porušujúca všeobecne bezpečnosť informačného systému, konkrétne niektorú zásadu bezpečnostnej politiky alebo niektoré bezpečnostné opatrenie.

Dôsledok – straty ako výsledky naplnených hrozieb môžu byt' vyjadrené prostredníctvom jednej alebo viacerých oblasti dôsledkov. K základným oblastiam patrí zničenie, znemožnenie prístupu k službe, prezradenie a modifikácia.

Dôvernosť – údaj uložený v informačnom systéme resp. prenášaný sieťou má byť prístupný iba oprávneným osobám. Pod prístupom sa rozumie zobrazenie údaja, vytlačenie údaja i samotné zistenie faktu, že došlo k prenosu (uloženiu) údaja.

Hrozba – akcia alebo potenciálna akcia, ktorej výsledkom môže byt' degradácia: utajenia (kompromitácia), celistvosti (narušenie integrity) alebo dostupnosti (znemožnenie prístupu k službe) systému alebo siete.

Identifikácia a autentifikácia – zabezpečujú určenie a overenie identity používateľa. Identifikácia a autentifikácia umožňuje účtovateľnosť aktivít používateľov (napríklad spätnej kontroly prihlasovania sa a odhlasovania sa do systému) ako aj evidencie aktivít používateľov v systéme.

Chránená miestnosť je osobitne určená samostatná miestnosť, ktorá je stavebne alebo inak fyzicky oddelená od zvyšku chráneného priestoru alebo od nechránených priestorov.

Osobný údaj - osobnými údajmi sú údaje týkajúce sa identifikovanej fyzickej osoby alebo identifikovateľnej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora.

Informačný systém osobných údajov - je akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe.

Spracovanie osobných údajov / obmedzenia - spracúvaním osobných údajov sa rozumie spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi, alebo so súbormi osobných údajov, najmä získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, zmena. Obmedzením spracúvania osobných údajov je označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti.

Dotknutá osoba – dotknutou osobou je každá fyzická osoba, ktorej osobné údaje sa spracúvajú.

Profilovanie - profilovaním je akákoľvek forma automatizovaného spracúvania osobných údajov spočívajúceho v použití osobných údajov na vyhodnotenie určitých osobných znakov alebo charakteristík týkajúcich sa fyzickej osoby.

Šifrovanie - šifrovaním sa rozumie transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra ako je kľúč, alebo heslo.

Logovanie – logom sa rozumie záznam o priebehu činnosti používateľa v automatizovanom informačnom systéme.

Článok I
ÚVODNÉ USTANOVENIA

(1) Zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti sa do slovenského právneho poriadku transponuje smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (ďalej aj len „Smernica“). Cieľom Smernice, rovnako ako aj zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti, je zaistiť ochranu informačných systémov a sietí pred narušením buď samotných technických zariadení, alebo údajov, ktoré sa v nich spracovávajú, alebo služieb, ktoré sa pomocou nich poskytujú.

(2) Fakultná nemocnica s poliklinikou Nové Zámky (ďalej len „FNsP“), patrí podľa §17 Zákona č. 69/2018 Z. z. medzi prevádzkovateľov základnej služby, a preto je povinná do 24 mesiacov odo dňa oznámenia o zaradení do registra prevádzkovateľov základných služieb prijať a dodržiavať všeobecné bezpečnostné opatrenia najmenej v rozsahu bezpečnostných opatrení podľa § 20 a sektorové bezpečnostné opatrenia, ak sú prijaté.

(3) FNsP je prevádzkovateľom základnej služby podľa § 3 písm. k) prvý bod zákona 69/2018 o kybernetickej bezpečnosti v sektore Zdravotníctvo, podsektor Zdravotnícke zariadenia v pôsobnosti ústredného orgánu – Ministerstva zdravotníctva SR.

Článok II
CHRÁNENÁ MIESTNOSŤ IT

(1) Je osobitne určená samostatná miestnosť, ktorá je stavebne alebo inak fyzicky oddelená od zvyšku chráneného priestoru alebo od nechránených priestorov, pričom slúži najmä na centralizovanie aktív a systematické uchovávanie osobných údajov v akejkoľvek elektronickej, písomnej alebo inej forme; za chránenú miestnosť môže byť považovaný aj osobitne zabezpečený odkladací priestor (napr. trezor, iné pevné uzamykateľné priestory); do chránenej miestnosti je regulovaný fyzický prístup zamestnancov a iných osôb a je vo zvýšenej miere zabezpečená prijatím vhodných technických bezpečnostných opatrení, realizovaných prostriedkami fyzickej povahy.

(2) Ochrana chránených priestorov IT (CHP_IT)

Kancelárie:	
Označenie miestnosti:	Číselné označenie a spravidla pri kanceláriách aj označenie zamestnancov využívajúcich chránenú miestnosť titulom, menom, priezviskom a funkciou v organizácii.
Počet vstupných dverí:	Každá chránená miestnosť má vlastné vstupné dvere.

Konštrukcia dverí:	Pevné, uzamykateľné.
Zabezpečenie vstupných dverí:	Zabezpečené pridelením kľúča, v priebehu noci sú zamknuté.
Zabezpečenie okien:	Okná nie sú zabezpečené zvýšenou mechanickou ochranou.
Ochrana vstupu v pracovnej dobe:	Prístup je umožnený len príslušným pracovníkom IT alebo personálnych útvarov, cudzie osoby môžu do miestnosti vstupovať len v sprievode.
Bezpečnostné opatrenia:	Ochrana objektu, dostatočné zabezpečenie vstupu do chránených priestorov, obmedzenie prístupu do kancelárie iba pre konkrétneho zamestnanca.
Serverovňa:	
Označenie miestnosti:	Bez označenia
Počet vstupných dverí:	Jedny
Konštrukcia dverí:	Pevné, uzamykateľné.
Zabezpečenie vstupných dverí:	Kľúče má úzky okruh osôb.
Zabezpečenie dverí do Serverovne:	Áno, uzamykateľné so zabezpečením prístupu len pre určené osoby.
Zabezpečenie okien:	Okná sú zabezpečené zvýšenou mechanickou ochranou .
Zabezpečenie priestoru serverovne:	Priestor zabezpečený kamerovým systémom, požiarnym hlásičom.
Zabezpečenie teploty v serverovni:	Priestor klimatizovaný na konštantnú teplotu. 1x ročne servisné práce na klimatizačnej jednotke zamestnancami FNsP.
Ochrana vstupu v pracovnej dobe:	Nepovolané osoby smú do serverovne vstupovať len v sprievode oprávnených osôb spoločnosti.
Bezpečnostné opatrenia:	Ochrana objektu, dostatočné zabezpečenie vstupu do chránených priestorov, obmedzenie prístupu do chránenej miestnosti – serverovňa len na nevyhnutný okruh oprávnených osôb spoločnosti a ďalších fyzických osôb zabezpečujúcich údržbu a technickú podporu v sprievode oprávnených osôb.
Vlastní zamestnanci:	Iba pracovníci oddelenia IT bez obmedzenia.
Zamestnanci externých dodávateľov:	Pohyb pod dohľadom zodpovedného zamestnanca
Upratovacia služba:	NIE – nemá prístup
Návštevy:	NIE – nemá prístup
Kontrola pohybu v CHP	
Vlastní zamestnanci:	Bez obmedzenia v rámci pridelených oprávnení a kľúčov od miestností, v ktorých vykonávajú pracovné činnosti.
Zamestnanci externých dodávateľov:	Pohyb výlučne pod dohľadom povereného zamestnanca spoločnosti.
Upratovacia služba:	Do niektorých chránených miestností mu môže byť odmietnutý prístup (napr. serverovňa).
Správca budovy:	Iba na základe vopred oznámenej žiadosti a za prítomnosti povereného zamestnanca spoločnosti.
Primárne RACK-y	
Označenie miestnosti:	Bez označenia
Počet vstupných dverí:	Jedny
Konštrukcia dverí:	Pevné, uzamykateľné.
Zabezpečenie vstupných	Kľúče má úzky okruh osôb.

dverí:	
Zabezpečenie dverí:	Áno, uzamykateľné so zabezpečením prístupu len pre určené osoby.
Zabezpečenie okien:	Okná sú zabezpečené zvýšenou mechanickou ochranou resp. vo výškovej budove bez prístupu z balkóna.
Zabezpečenie teploty:	Priestor klimatizovaný na konštantnú teplotu. 1x ročne servisné práce na klimatizačnej jednotke zamestnancami FNsP.
Ochrana vstupu v pracovnej dobe:	Nepovolané osoby smú do priestorov vstupovať len v sprievode oprávnených osôb spoločnosti.
Bezpečnostné opatrenia:	Ochrana objektu, dostatočné zabezpečenie vstupu do chránených priestorov len na nevyhnutný okruh oprávnených osôb spoločnosti a ďalších fyzických osôb zabezpečujúcich údržbu a technickú podporu v sprievode oprávnených osôb.
Vlastní zamestnanci:	Iba pracovníci oddelenia IT bez obmedzenia.
Zamestnanci externých dodávateľov:	Pohyb pod dohľadom zodpovedného zamestnanca
Upratovacia služba:	NIE – nemá prístup
Návštevy:	NIE – nemá prístup
Sekundárne RACK-y	Umiestnené na uzavretých z pracoviskách so stálou službou 24/7
Označenie miestnosti:	Bez označenia
Počet vstupných dverí:	Niekoľko na jednotlivé pracoviská, otvárajú ich zvnútra zamestnanci
Zabezpečenie vstupných dverí:	Zvonku sa otvárajú len na kľúč
Zabezpečenie okien:	Okná na vyššom poschodí, mimo dosahu balkónov.
Ochrana vstupu v pracovnej dobe:	Nepovolané osoby smú do miestnosti vstupovať len v sprievode oprávnených osôb spoločnosti.
Bezpečnostné opatrenia:	Ochrana objektu, dostatočné zabezpečenie vstupu do chránených priestorov, obmedzenie prístupu do chránenej miestnosti len na nevyhnutný okruh oprávnených osôb spoločnosti a ďalších fyzických osôb zabezpečujúcich údržbu a technickú podporu v sprievode oprávnených osôb.
Vlastní zamestnanci:	Iba pracovníci oddelenia IT technici.
Zamestnanci externých dodávateľov:	Pohyb pod dohľadom zodpovedného zamestnanca.
Upratovacia služba:	Do niektorých chránených miestností mu môže byť odmietnutý prístup
Návštevy:	Pohyb výlučne pod dohľadom povereného zamestnanca spoločnosti.

Článok III

POLITIKA POUŽÍVANIA IT

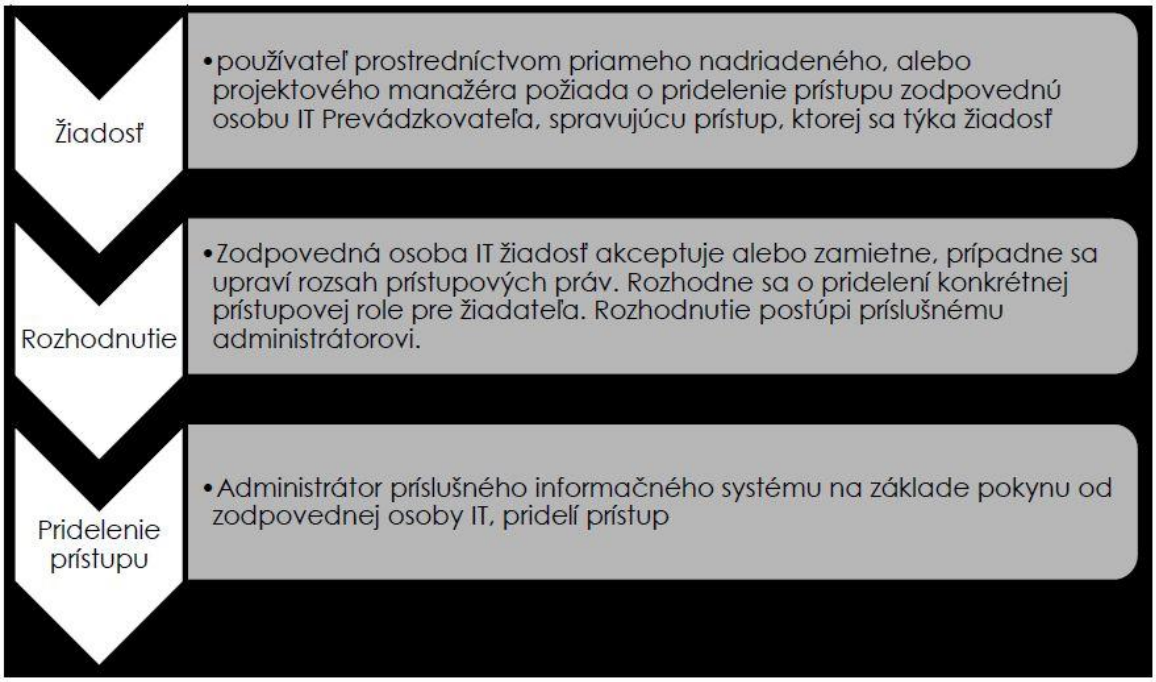
(1) **Správca siete IT**

a) Inštaluje systémové programy (predovšetkým operačné systémy).

b) Manipuluje s diskovými médiami a tlačiarňami.

c) Je zodpovedný za plnú prevádzkyschopnosť systémových prostriedkov a nástrojov.

d) Na základe povolení zriaďuje nové používateľské kontá, prideľuje pre ne základné prístupové práva, preveruje oprávnenosť prístupových práv a používateľských kont a na základe povolenia ruší používateľské kontá. Faktické pridelenie prístupového práva je vždy sprevádzané nasledovným procesom:



Vzor tlačiva tvorí prílohu č. 2 tejto smernice. V niektorých prípadoch, po zhodnotení pracovníkmi OINF, môže byť požadovaný okrem podpisu priameho nadriadeného aj súhlas štatutárov nemocnice.

e) Zodpovedá za zálohovanie a archiváciu systémových a používateľských dát, za archív a vedenie evidencie záložných médií a ich bezpečné uloženie.

f) Pravidelne kontroluje stav technických súčastí informačného systému.

g) Raz týždenne nastavuje a kontroluje stav serverov.

h) Podľa požiadaviek bezpečnostnej politiky nastavuje prístupové práva na aktívnych sieťových prvkoch a komunikačných zariadeniach.

i) Pravidelne monitoruje stav siete pomocou programových nástrojov pre riadenie siete.

j) Udržuje v aktuálnom stave informácie o topológii siete, aktívnych a pasívnych prvkoch, o ich parametroch a nastaveniach.

k) Zriaďuje, eviduje a ruší kontá používateľov a skupín, pravidelne preveruje oprávnenosť používateľských kont, prípadne prístupových práv.

l) Vykonáva pravidelný audit databáz a pravidelne ich vyhodnocuje a zálohuje.

m) Uskutočňuje pravidelnú údržbu databáz, monitorovanie ich priestorových nárokov, optimálne nastavovanie parametrov databáz v závislosti od stavu operačného systému a od aktuálnej situácie v databázach.

n) Rieši havarijné stavy podľa havarijného poriadku, obnovuje dáta, funkčnosť databáz a konzultuje neštandardné stavy s dodávateľskými firmami.

o) Testuje a nasadzuje nové databázové softvéry, prípadne ich update a upgrade.

p) Zálohuje databázy a kontroluje pravidelnosť a spoľahlivosť prevádzky z hľadiska obnovy databáz po poškodení dát a obnovy databáz k dátumu.

q) Archivuje systémové a používateľské dáta databáz a vedie evidenciu záložných médií a archívu.

r) Kontroluje v logovacích súboroch oprávnenosť vstupu do databázy (ochrana pred neoprávneným vstupom), zisťuje či bola prekonaná bezpečnostná brána a v prípade, že bola prekonaná, preveruje postup jej prekonania.

s) Spolupracuje s ostatnými oddeleniami pri testovaní, výberovom konaní pre nový softvér. Tvorí a spolupodieľa sa na tvorbe návrhov smerníc, upresnení a školení súvisiacich s bezpečnosťou informačných systémov.

t) Nastavuje bezpečnostné charakteristiky pre jednotlivé komponenty informačného systému vrátane komunikačných prvkov.

u) Vyhodnocuje a spravuje kontrolné záznamy.

v) Vykonáva bezpečnostné školenia používateľov.

w) Kontroluje fyzickú bezpečnosť počítačového vybavenia a hlavnej miestnosti (serverovne), archívnych médií a výstupných zariadení (tlačiarne, zapisovače, atď.).

x) Kontroluje prístup k zariadeniam systému. Kontroluje bezpečné uloženia záložných médií a archívov.

y) Povoľuje zavedenie nových používateľov.

z) Kontroluje a spravuje systém prihlasovania užívateľov a stanovuje maximálnu dobu životnosti hesiel podľa bezpečnostnej politiky.

aa) Riadi a zabezpečuje päťročnú archiváciu súborov týkajúcich sa bezpečnostných záznamov operačného systému a dôležitých aplikácií.

bb) Analyzuje prieniky do informačných systémov, vytvára, optimalizuje a spravuje bezpečnostnú politiku.

(2) **Technik IT**

a) Odstraňuje technické poruchy a závady na zariadeniach IT a to buď svojpomocne, napr. výmenou súčiastky, časti dielu alebo celého dielu za nový v rámci záručných podmienok, alebo formou doručenia chybného zariadenia do príslušného servisného strediska alebo dohovoru o oprave cez dodávateľa daného zariadenia.

b) Realizuje technické prepojenia lokálnych počítačových sietí na súčastiach a pracoviskách.

c) Pripája zariadenia IT do elektrickej siete napájania a do počítačovej siete. Prepája jednotlivé zariadenia IT medzi sebou.

d) Vykonáva previerku zariadení IT, ktoré podliehajú pravidelnému technickému auditu.

(3) **Používateľ IT**

a) Používa PC, operačný systém na ňom nainštalovaný, ako aj všetky aplikácie, na ktoré dostal oprávnenie.

b) Prihlasuje sa do počítačovej siete a používa zdielané súbory, databázy, aplikácie, tlačiarne, či iné zariadenia podľa práv, ktoré mu boli pridelené jeho priamym nadriadeným.

c) Je preukázateľne poučený o povinnosti dodržiavať túto smernicu a riadiť sa ňou pri svojej práci.

d) Riadi sa pokynmi zamestnancov OINF a obracia sa na nich v prípade závad, porúch a mimoriadnych situácií.

e) Dbá na ochranu spracovávaných dát.

f) PC a ostatné zariadenia IT používa výhradne na služobné účely vyplývajúce z jeho popisu pracovnej činnosti.

g) Na iné účely použitia zariadení IT potrebuje písomný súhlas priameho nadriadeného.

h) Používatelia sú povinní chrániť prístupové heslá k informačnému systému (IS), operačnému systému (OS), pošte, vzdialenému prístupu a iným heslom chráneným prístupom.

i) IT zariadenia sú k perifériám zverené bez obmedzovania prístupu a bez obmedzenia internetu, pričom sa predpokladá, že používateľ si je po zaškolení vedomý rizík vyplývajúcich z používania tohto zariadenia.

j) IT technika obsahuje antivírový softvér (SW), ktorý sa sám aktualizuje a aktualizácie OS sa preberajú a inštalujú automaticky.

k) V prípadne upozornenia používateľa na spustenie aktualizácie OS, je nutné túto aktualizáciu v čo najbližšom možnom čase vykonať.

l) Pri akejkoľvek zmene týkajúcej sa používateľa IT a majúcej vplyv na používanie softvéru je povinný jeho priamy nadriadený formou požiadavkového listu požiadať o vykonanie tejto zmeny na OINF.

(4) **Používateľ Internetu**

Používateľom internetu je zamestnanec prevádzkovateľa, ktorému bolo pridelené používateľské konto, resp. iným spôsobom umožnený prístup do celosvetovej počítačovej siete Internet (www).

(5) **Používateľ Intranetu**

Používateľom intranetu je zamestnanec prevádzkovateľa, ktorému bolo pridelené používateľské konto a heslo (centrálne vytvorené jedno konto a heslo pre používateľov) na základe toho umožnený prístup do Intranetu počítačovej siete (tzv. vnútro-podnikovej siete).

(6) **Používateľ elektronickej pošty**

Používateľom elektronickej pošty je zamestnanec prevádzkovateľa, ktorému bolo pridelené používateľské konto a na základe toho umožnené používanie elektronickej pošty (e-mailu).

(7) **Používateľ elektronickej registratúry**

Používateľom elektronickej registratúry je zamestnanec prevádzkovateľa, ktorému bolo pridelené používateľské konto a na základe toho umožnené používanie elektronickej registratúry (systém registratúry).

(8) **Zamestnanec**

Pre účely tejto smernice sa za zamestnanca považujú všetci kmeňoví zamestnanci prevádzkovateľa, ale aj externí zamestnanci, ktorí majú s prevádzkovateľom pracovno-

právny vzťah, prípadne iný zmluvný vzťah. Na vstup do IS je každému pridelené prihlasovacie meno a heslo.

Článok IV
POUŽÍVANIE HARDVÉRU

(1) Na pracoviskách prevádzkovateľa sa používa iba taký hardvér, ktorý je schválený príslušnými vedúcimi zamestnancami a je evidovaný v evidencii majetku na oddelení správy majetku ekonomického odboru.

(2) Akýkoľvek iný hardvér sa zakazuje používať.

(3) Zakazuje sa akýkoľvek zásah do hardvéru alebo jeho konfigurácie a jeho svojvoľné premiestňovanie či výmena. Touto činnosťou je poverený zamestnanec OINF, ktorý túto činnosť vykoná.

(4) Používatelia IT, ktorým boli zverené alebo zapožičané prenosné notebooky, telefóny, prípadne akékoľvek iné zariadenia IT, sú povinní s nimi nakladať tak, aby nedošlo k ich strate, zneužitiu či krádeži, nesmú ich požičať, prenechať, odovzdať tretej osobe, či u tretej osoby takéto zariadenie založiť formou záložného práva.

(5) Poruchu hardvéru treba nahlásiť OINF. Pracovník oddelenia OINF sa okamžite, prípadne podľa dohody postará o nápravu, opravu alebo výmenu poruchového hardvéru.

(6) Kľúčové servery IS sú umiestnené v klimatizovanej serverovni. Len servery, ktoré sa používajú aj ako pracovné stanice sú umiestnené na pracoviskách nemocnice.

(7) Správa serverov je rozdelená medzi pracovníkov OINF podľa druhu IS, ktorý sa na nich prevádzkuje.

(8) Servery sú k elektrickému rozvodu pripájané cez UPS záložné zdroje, ktoré sú ešte proti dlhodobejšiemu výpadku napájania chránené dieselagregátmi.

(9) Správa serverov, IS je krytá aj supervíziou dodávateľských firiem programového vybavenia IS. Pravidelne sa vykonávajú aktualizácie OS aj programov a číselníkov IS na serveroch.

(10) Kontrola dátových diskov aj antivírová kontrola sa vykonáva podľa plánu kontrol.

(11) Zálohovanie sa vykonáva v čase mimo pracovnej doby, prípadne v čase najnižšieho používania a to dvojúrovňovo. Prvá záloha sa ukladá na vnútorný disk servera, ale nie na disk, kde je umiestnená databáza IS. Druhá záloha sa vytvorí po ukončení zálohovania, kopírovaním zálohy na archívny NAS server. Tým sa zároveň kontroluje aj jej použiteľnosť.

(12) Zálohy databáz IS sa archivujú na samostatných NAS serveroch s vysokou kapacitou diskového priestoru. Obsahujú RAID5 kedy porucha jedného disku nespôsobí stratu dát. Umiestnené sú v serverovniach s klimatizáciou a v inej budove ako server a databáza IS.

(13) Zálohy databáz sa udržujú v archíve minimálne týždeň, okrem toho u najdôležitejších IS sa archivuje aj niekoľko mesačných záloh.

(14) Snímky, štúdie z RDG pracovísk, CT a MRI sa ukladajú na diskové pole s vysokou kapacitou a sú on-line prístupné od začiatku digitálneho ukladania snímok a štúdií. Zálohujú sa automaticky na magnetické kazetové pásky vysokej kapacity značené jedinečným čiarovým kódom pomocou robotizovanej páskovej mechaniky vždy dvojmo na dve rôzne kazetové pásky. Zaplnené kazety sa archivujú v plechových uzamknutých skriniach mimo najbližšieho okolia serverovne.

Článok V
POUŽÍVANIE SOFTVÉRU

(1) Pri práci s PC je zakázané pracovať s iným softvérom, než aký bol nainštalovaný, resp. schválený (unifikovaný).

(2) Používateľ IT používa len taký softvér, na ktorého používanie má podľa schválenia nárok.

(3) Pri akejkoľvek zmene týkajúcej sa používateľa IT, ktorá má vplyv na používanie softvéru, je používateľ IT povinný požiadať príslušného nadriadeného o vykonanie takejto zmeny.

(4) Po zakúpení softvéru tento nový softvér inštaluje zamestnanec OINF, alebo zamestnanci dodávateľskej firmy za prítomnosti zamestnanca OINF.

(5) Poruchu softvéru treba nahlásiť Odboru informatiky.

(6) Pracovník OINF sa okamžite, prípadne podľa dohody postará o nápravu poruchy softvéru.

(7) Zakazuje sa používať, uchovávať alebo distribuovať akýkoľvek pirátsky softvér a údaje na hardvérovom vybavení.

(8) Pracovné stanice sú zapojené do Activ Directory, ktorá umožňuje administrátorom nastavovať politiku, inštalovať programy na mnoho počítačov alebo aplikovať kritické aktualizácie v celej organizačnej štruktúre. Active Directory svoje informácie a nastavenia ukladá v centrálnej organizovanej databáze. Umožňuje niektorým užívateľom dať väčšie práva, iným menšie.

Článok VI
POUŽÍVANIE SLUŽIEB INTERNETU, INTRANETU A ELEKTRONICKEJ POŠTY A ELEKTRONICKEJ REGISTRATÚRY

(1) Prevádzkovateľ používa alebo môže používať softvér a systémy, ktoré umožňujú monitorovať a zaznamenávať všetky použitia celosvetovej počítačovej siete Internet a elektronickej pošty. Systémy môžu zaznamenávať prístup na webové stránky, diskusné skupiny, použitie elektronickej pošty, prenos súborov medzi prevádzkovateľom a inými subjektami.

(2) Používateľ Internetu a elektronickej pošty musí vedieť, že prevádzkovateľ má právo v súlade s platnou legislatívou preverovať použitie týchto prístupov.

(3) Prevádzkovateľ má právo nariadiť kontrolu všetkých dát a akýchkoľvek súborov, ktoré sú uložené na lokálnych diskoch PC používateľov IT, alebo v ich domovských adresároch na serveroch prevádzkovateľa.

(4) Zakazuje sa zobrazovanie, archivovanie, uchovávanie, rozširovanie, spracovávanie alebo zaznamenávanie akéhokoľvek obrázku, či dokumentu s jednoznačným sexuálnym obsahom.

(5) Zakazuje sa používať elektronickú poštu na posielanie, preposielanie a rozširovanie pošty zábavného charakteru a charakteru, ktorý priamo nesúvisí s výkonom pracovnej činnosti.

(6) Prístup na Internet a elektronickú poštu sa nesmú vedome použiť na porušenie všeobecne záväzných právnych predpisov Slovenskej republiky alebo medzinárodných zmlúv, ktorými je Slovenská republika viazaná.

(7) Akýkoľvek softvér alebo súbor získaný prostredníctvom Internetu a uložený na lokálnej sieti prevádzkovateľa, alebo na lokálnom disku používateľa IT, sa stáva majetkom prevádzkovateľa. Všetky takéto súbory, dokumenty alebo softvér, sa môžu používať výhradne spôsobom, ktorý je v súlade s udelenými licenciami, autorskými právami, resp. ich odsúhlasil útvar OINF a musia priamo súvisieť s pracovnými povinnosťami používateľa IT.

(8) Zakazuje sa získavanie a následné ukladanie zábavného softvéru alebo hier, videí, obrázkov a zvukových súborov z Internetu alebo prostredníctvom elektronickej pošty, hranie hier na Internete. Takisto sa zakazuje rozširovanie akéhokoľvek softvéru či údajov, ktoré sú majetkom prevádzkovateľa bez jeho predchádzajúceho písomného súhlasu.

(9) Používateľom Internetu a elektronickej pošty sa zakazuje využívať svetovú počítačovú sieť Internet a elektronickú poštu na zámerné rozširovanie akýchkoľvek vírusov, červov, trójskych koňov alebo iného škodlivého softvéru. Takisto používateľ nesmie využiť či zneužiť prístup na Internet či elektronickú poštu na vyradenie, preťaženie alebo oklamanie akéhokoľvek počítačového systému alebo počítačovej siete a tým narušiť súkromie alebo bezpečnosť iného používateľa či spoločnosti.

(10) Vyjadrovať sa v mene prevádzkovateľa, alebo jeho súčastí do akýchkoľvek diskusných skupín môžu len zamestnanci, ktorí sú riadne poverení komunikáciou s médiami. Ostatní používatelia Internetu a elektronickej pošty sa môžu zúčastňovať na diskusiách a fórach v priebehu pracovnej doby, ak sa to vzťahuje na ich odbornú činnosť, ale v tom prípade vystupujú ako jednotlivci vo vlastnom mene a sú povinní informovať ostatných zúčastnených, že nie sú oprávnení vystupovať v mene prevádzkovateľa, alebo jeho súčastí. Pri účasti v týchto diskusiách a fórach je používateľ Internetu a elektronickej pošty povinný zdržať sa akýchkoľvek politických, náboženských, rasových prejavov, prejavov neznášanlivosti a prejavov urážajúcich ľudskú dôstojnosť, či prejavov týkajúcich sa trestnej činnosti.

(11) Používateľ Internetu, intranetu a elektronickej pošty nesmie zverejňovať údaje a dôverné informácie o prevádzkovateľovi. Používatelia Internetu a elektronickej pošty

môžu počas obedovej alebo inej prestávky, alebo po pracovnej dobe využívať prístup na Internet a elektronickú poštu pre prieskum alebo prezeranie informačných zdrojov nesúvisiacich s náplňou práce len za predpokladu, že budú dodržané všetky ustanovenia tejto smernice a so súhlasom priameho nadriadeného. Porušenie tohto ustanovenia je závažným porušením pracovnej disciplíny a má za následok okamžité skončenie pracovného pomeru zamestnanca.

(12) Prevádzkovateľ je v zmysle príslušných zákonných ustanovení povinný poskytnúť orgánom činným v trestnom konaní všetky dostupné záznamy týkajúce sa prístupu na Internet, intranet a elektronickú poštu príslušného používateľa Internetu a elektronickej pošty.

(13) Používateľ Internetu a elektronickej pošty sa musí riadiť všeobecne záväznými právnymi predpismi, autorským právom, či obchodnými značkami.

(14) Komerčné používanie Internetu na podporu vedľajšej podnikateľskej činnosti prevádzkovateľa alebo jeho súčastí mimo jeho pracovnej náplne nie je možné.

(15) Používateľ elektronickej registratúry má vlastný účet do registratúry a heslo s ktorým sa prihlasuje do systému.

(16) Zamestnanci podateľne majú právo prezerať, skenovať, archivovať všetku prijatú poštu vo FNsP.

Článok VII
NARUŠENIE TECHNICKO – SOFTVÉROVEJ BEZPEČNOSTI

(1) Odbor informatiky zabezpečuje správu, údržbu, servis a ďalšie činnosti spojené s prevádzkovaním IS vo FNsP, rieši všetky požiadavky obsluhy, prijíma informácie o poruchách aj bezpečnostných incidentoch.

(2) Každý IS prevádzkovaný OINF má určeného pracovníka – správcu, ktorý zodpovedá za prevádzku IS vrátane ochrany údajov.

(3) Zamestnanec pri podozrení z narušenia bezpečnosti zvereného počítača upovedomí o tejto skutočnosti OINF a spolupracuje s jeho zamestnancami na náprave.

(4) Pri odstraňovaní porúch kľúčových komponentov IS je pracovník OINF oprávnený vyhlásiť technickú odstávku na nevyhnutný čas potrebný na odstránenie poruchy.

(5) Bezpečnosť databáz a aplikácií IS zabezpečujú poverení pracovníci OINF v spolupráci s poverenými pracovníkmi pracovísk.

(6) Riešenie nepredvídaných udalostí IS

a) stála služba OINF - nepretržitý pobyt na pracovisku počas pracovnej doby 7.00 – 15.00 je štandardne zabezpečený

b) pohotovostná služba OINF - 15,00 – 20,00 hod. v pracovných dňoch zabezpečuje kontrolu prevádzky informačných systémov, bezpečnosť uložených dát, rieši akútne poruchy, vykonáva stanovené testy, zálohy, antivírové kontroly, profylaktiku siete a serverov

c) pohotovostná služba OINF na telefóne v dňoch pracovného voľna a pokoja - 7,00 – 20,00 hod. rieši akútne problémy užívateľov telefonickou konzultáciou alebo osobným príchodom na miesto poruchy s následnými opatreniami na odstránenie chýb, zabránenie poškodeniu alebo úniku osobných údajov.

(7) V prípade nepredvídanej situácie je službu konajúci pracovník OINF oprávnený – podľa možnosti po predchádzajúcom upozornení užívateľov – vyhlásiť technickú odstávku systému na nevyhnutný čas potrebný pre riešenie udalosti.

(8) V prípade výskytu bezpečnostného incidentu pracovníci ihneď informujú povereného pracovníka pracoviska, prípadne povereného pracovníka OINF, s ktorým tiež konzultujú postup riešenia incidentu.

(9) Riešenie každého bezpečnostného incidentu musí byť primerane zdokumentované, a to povereným pracovníkom príslušného pracoviska alebo pracovníkom OINF . Dokumentuje sa predovšetkým príčina vzniku incidentu (pokiaľ je známa), dôsledky, všetky opatrenia prijaté pri riešení incidentu a ich účinnosť, ako aj zistené nedostatky v existujúcom pláne pre prípad nepredvídanej situácie.

(10) Priority pri riešení bezpečnostného incidentu:

a) bezodkladné obnovenie bežnej prevádzky IS aspoň v núdzovom režime, zabezpečenie ochrany údajov, zachovanie dôkazového materiálu nevyhnutného na ďalšiu analýzu príčin vzniku bezpečnostného incidentu,

b) zistenie príčin, ktoré viedli k vzniku bezpečnostného incidentu,

c) určenie zodpovednosti za vznik bezpečnostného incidentu a vyvodenie dôsledkov,

d) zovšeobecnenie zistených skutočností a návrh opatrení na zabránenie opakovanému výskytu bezpečnostného incidentu.

(11) Preventívne opatrenia

a) Pracovníci OINF alebo poverená externá dodávateľská firma sú povinní pravidelne vykonávať základnú preventívnu kontrolu kľúčových komponentov IS (testovanie systému, odstránenie nepotrebných súborov, posúdenie rýchlosti zapĺňania pamäťovej kapacity, množstvo a vek životnosti médií používaných na zálohovanie, previerka na výskyt nových programov v systéme, vyčistenie komponentov systému a podobne). Na tento účel je možné vyhlásiť odstávku systému na nevyhnutne potrebnú dobu. Termín odstávky stanoví tak, aby čo najmenej narušil bežnú činnosť pracovísk a užívateľov o tomto termíne oboznámia s dostatočným predstihom.

b) Pracovníci OINF sú povinní pravidelne vykonávať základnú preventívnu kontrolu zameranú na preverenie funkčnosti komponentov nevyhnutných pre riešenie nepredvídaných situácií (zariadenie pre zálohovanie a obnovu údajov, médiá so záložnými kópiami údajov a programov, UPS, aktuálnosť zálohovaných prístupových hesiel a ďalších uchovávaných parametrov systému).

c) Pracovníci OINF pomáhajú používateľom IS na jednotlivých pracoviskách riešiť problémy, ktoré sa objavia pri práci so systémom. V prípade opakovaného výskytu problémov z dôvodu nedostatočnej kvalifikácie, resp. schopností užívateľa pracovať s IS, je vedúci odboru informatiky oprávnený upozorniť nadriadeného príslušného používateľa na zistené nedostatky a potrebu nápravy.

(12) Centrálne servery IS - Prístup do priestorov centrálneho servera IS majú len správcovia a riaditelia FNsP, ostatné osoby sa môžu v týchto priestoroch zdržiavať len so súhlasom vedúceho OINF alebo riaditeľa FNsP.

(13) Antivírová ochrana - v prípade, že sa na pracovnej ploche užívateľa zobrazí varovanie, že sa na zariadení nachádza vírus, užívateľ nesmie toto varovanie ignorovať. V prípade zavírenia pevného disku, USB kľúča a pod., užívateľ túto skutočnosť bezodkladne oznámi pracovníkom OINF, prípadne po konzultácii s nimi vykoná antivírovú „dezinfekciu“ príslušného pamäťového média. V prípade objavenia vírusu v prijatej elektronickej pošte užívateľ bezodkladne o tejto udalosti upovedomí pracovníkov OINF. V žiadnom prípade zavírenú elektronickú poštu neposiela inému

adresátovi, a na svojej pracovnej stanici ju uschová len dočasne a len na žiadosť pracovníka OINF (na účely ďalšej analýzy prieniku vírusu do systémovo FNsP).

(14) Užívateľ pracovnej stanice zaznamená a pracovníkom OINF ohlási každú odchýlku od bežnej činnosti pracovnej stanice, predovšetkým nasledovné udalosti:

a) hlásenia chýb operačného systému a aplikácií, s ktorými používateľ pracuje (presný prepis chybového hlásenia) spolu so stručným popisom situácie (vykonávaných akcií), počas ktorej sa toto hlásenie vyskytlo,
b) problémy s technickými zariadeniami pracovnej stanice spolu s popisom situácie, počas ktorej k problémom došlo (popis akcií, zadávaných údajov alebo viditeľných javov, ktoré predchádzali, resp. nasledovali výskyt problému).

(15) Užívateľ pracovnej stanice zaznamená a svojmu nadriadenému a následne vedúcemu OINF bezodkladne ohlási každú udalosť, ktorá by mohla indikovať porušenie bezpečnosti IS, predovšetkým však nasledovné udalosti:

a) výskyt vírusu (prepis varovného hlásenia),
b) únik údajov, s informáciou, aké informácie unikli, kam a ako,
c) odcudzenie médií s údajmi z pracovnej stanice,
d) odcudzenie technických zariadení pracovnej stanice,
e) neoprávnený zásah do technických zariadení pracovnej stanice,
f) neoprávnený zásah do programového vybavenia pracovnej stanice (vrátane výskytu nových súborov alebo adresárov na disku pracovnej stanice) alebo do nastavenia jeho parametrov (napr. nastavené zdieľanie disku alebo adresárov pracovnej stanice).
g) Vyššie uvedené zásady platia aj v prípade, že užívateľ dočasne používa pracovnú stanicu pridelenú inému užívateľovi; v takom prípade naviac informuje aj užívateľa, ktorému bola pracovná stanica pridelená.

(16) Užívatelia sú povinní spolupracovať s povereným pracovníkom pracoviska, ako aj s pracovníkmi OINF pri objasňovaní príčin výskytu bezpečnostných problémov, aby mohli byť následne vykonané opatrenia, ktoré by zabránili výskytu podobnej situácie.

(17) Používateľ internetu, intranetu, elektronickej pošty a elektronickej registratúry je povinný zachovávať mlčanlivosť o informáciách získaných zo zdrojov FNsP NZ.

Porušenie tohto ustanovenia je závažným porušením pracovnej disciplíny a má za následok okamžité skončenie pracovného pomeru zamestnanca.

Článok VIII
PREVENTÍVNE OPATRENIA PROTI NARUŠENIU TECHNICKO – SOFTVÉROVEJ BEZPEČNOSTI

(1) Havárie IS spôsobené technickou chybou niektorého komponentu centrálneho počítača – serveru, preventívne opatrenia:

a) zabezpečiť záložné zdroje s automatickým shutdownom,
b) monitorovať činnosť serverov, kontrolovať chybové hlásenia,
c) v serveroch používať diskové polia s hotswap diskami,
d) zabezpečiť dostatok finančných prostriedkov na obnovu IS, podľa možnosti obmieňať server každé tri roky,
e) zachovávať pravidlo - novší server sa stáva hlavným a starší záložným
f) zálohovať,

(2) Vírusová infiltrácia –preventívne opatrenia:

a) zabezpečiť antivírovú ochranu,
b) inštalovať len autorizované programy oprávnenými zamestnancami,
c) preverovať cudzie nosiče (FD, CD ROM, USB...),
d) nepripájať nepreverené PC bez vedomia OINF do LAN,
e) nepoužívané pasívne rozvody odpojiť od aktívnych prvkov LAN,
f) neotvárať nevyžiadané e-mailové prílohy,
g) sledovať aktuálne dianie na LAN a v sieti internet,

(3) Neautorizovaný vstup z internetu – preventívne opatrenia:

a) nespúšťať programy z prostredia internetu nepodpísane certifikačnou autoritou,
b) nesťahovať neautorizované programy z prostredia internetu,
c) kontrolovať a vyhodnotiť logy súborov firewallu, routerov, antivírového programu a pod.,
d) zabezpečiť súborovú integritu OS a obnovu poškodených alebo infikovaných údajov zo záloh,

e) zvýšiť bezpečnosť firewallov,
f) nastaviť kryptované prenosy v LAN sieti,
g) pokiaľ existuje prístup z internetu do lokálnej siete, je nutné, aby bol vytvorený iba kryptovaným prenosom minimálne cez protokol SSH a nepoužívalo sa pre autorizáciu vstupov meno a heslo, ale privátne a verejné kľúče v minimálnej dĺžke 512 bite, optimálne 1024 bite, prípadne využiť zabezpečenú VPN
h) nainštalovať doplnkové programy , ktoré eliminujú možnosť napadnutia počítača.

(4) Technické narušenie, alebo zlyhanie bezpečnosti zariadenia v IS - pamäť počítača, procesor, CD/DVD-RW , harddisk , wifi zariadenie – hlásiť na OINF

(5) Porucha napájania, strata dodávky elektrickej energie - dôležité aktívne prvky siete je nutné chrániť záložnými zdrojmi elektrickej energie so stabilizátorom sieťového napätia,

(6) Porucha aktívnych prvkov siete - preventívne opatrenia:

a) monitorovať činnosť,
b) zabezpečiť dostatočnú kapacitu,
c) pripájať ich prostredníctvom záložného zdroja,
d) zabezpečiť dostatočnú ochranu pred nepovolaným prístupom.

(7) Porucha pasívnej časti siete - preventívne opatrenia: premerať kabeláž, zásuvky a konektory,

(8) Havária databáz - preventívne opatrenia:

a) sledovať konfiguračné súbory,
b) monitorovať hlásenia programov a včas na nich reagovať,
c) denne kontrolovať chybové hlásenia aplikácie a databázy,

(9) Havária aplikácie - preventívne opatrenia:

a) sledovať hlásenia aplikácie a zaznamenávať postrehy užívateľov,
b) sledovať konfiguračné súbory,
c) monitorovať hlásenia a včas na nich reagovať,
d) denne kontrolovať chybové hlásenia aplikácie,

(10) Porucha pracovných staníc - preventívne opatrenia:

a) používať len autorizované programy,
b) inštalovať antivírové programy,
c) inštalovať nové programy smie len poverený zamestnanec,
d) užívatelia nesmú zasahovať do konfiguračných súborov,
e) chybové hlásenia sú povinný hlásiť správcovi systému,
f) zálohovať dáta na určené média,
g) za zálohy, prevádzku a bezpečnosť zodpovedá užívateľ.

(11) Mimoriadne udalosti spôsobené vplyvom zvyškových rizík - preventívne opatrenia:

a) zabezpečiť niekoľkonásobné záložne kópie,
b) kontrolovať, či sú splnené protipožiarne opatrenia,
c) kontrolovať osoby pri vstupe do priestorov,
d) vo vybraných priestoroch inštalovať EZS, bezpečnostné mreže, dvere,
e) zabezpečiť autentizáciu osôb pri vstupe do chránených priestorov,
f) v prípade vyradenia aktív IS z činnosti zvolať krízový štáb,
g) koordinovať činnosť podľa bezpečnostných záverov,
h) aktivovať záložne pracovisko,
i) skontrolovať úplnosť systému na záložnom pracovisku,
j) spustiť záložnú prevádzku,
k) odstrániť škody na pôvodnom pracovisku,
l) po obnovení funkčnosti vrátiť činnosti na pôvodné pracovisko,
m) v prípade napadnutia len časti aktív IS: presunúť aktíva do vyhovujúcich priestorov, inštalovať záložné databázy a pripojenia ak sú nutné, spustiť prevádzku,
n) po odstránení dôsledkov vrátiť činnosť do stavu pred udalosťou.

Článok IX
VŠEOBECNÉ PRAVIDLÁ BEZPEČNOSTI IT

(1) Používateľ IT je oprávnený pracovať s počítačom, softvérom a údajmi potrebnými pre výkon jeho činnosti iba v súlade s pridelenými právami a oprávneniami.

(2) Je zakázané poskytovať tretím osobám špecifické informácie o používateľoch IS, ktoré by mohli byť zneužité pre neoprávnený prístup k údajom a programom, najmä identifikácie a autentifikácie, rozsah oprávnení a práv a heslá používateľov IT.

(3) Každý používateľ IT má pridelené svoje prihlasovacie meno a heslo, ktoré musí zachovať v tajnosti. Tieto mená a heslá pomáhajú stanoviť osobnú zodpovednosť. Zakazuje sa spoločné používanie prihlasovacích mien a hesiel viacerými používateľmi IT. V prípade nebezpečia prezradenia je potrebné tieto heslá okamžite zmeniť.

(4) Heslá sa menia pravidelne v 6 mesačných intervaloch. Používateľ je povinný pri zmene hesla dbať na jeho neprelomiteľnosť.

(5) Používateľ IT je plne zodpovedný za svoje heslo, nesmie byť ľahko uhádnuteľné, alebo odvoditeľné. V prípade zabudnutia hesla používateľom IT, si používateľ IT v súčinnosti so zamestnancom OINF dohodne nové heslo.

(6) V záujme zaistenia bezpečnosti svojich počítačov, počítačových sietí a softvérového vybavenia majú zamestnanci nainštalované rôzne programy (napr. firewall, proxy server, antivírusové prostriedky), monitorovacie systémy pre Internet a elektronickú poštu a bezpečnostné systémy. Zamestnancom sa zakazuje vyraďovať z činnosti, narúšať, prekonávať alebo obchádzať ktorékoľvek bezpečnostné zariadenie alebo systém.

(7) Svojvoľné zapájanie sieťových prvkov ako wifi routre, mobilný internet a pod., ktoré neboli písomne schválené OINF sa považuje za hrubé porušenie pracovnej disciplíny a napĺňa podľa ZoKB 69/2018 podstatu kybernetického útoku. Prevádzkovateľovi vzniká povinnosť takýto incident nahlásiť NBU, ktorá incident následne prešetrí.

(8) Sieťové prvky je oprávnený inštalovať, konfigurovať a zapájať výhradne zamestnanec OINF, alebo poverená firma za prítomnosti zamestnanca OINF.

(9) Súbory, ktoré obsahujú citlivé (dôverné) údaje, musia byť pri akomkoľvek prenose prostredníctvom Internetu zašifrované. V tomto smere bude používateľovi IT nápomocný zamestnanec OINF.

(10) Pri opustení pracoviska je potrebné vylúčiť akúkoľvek možnosť neoprávneného prístupu tretích osôb k dátam a manipuláciu s nimi. V prípade, že používateľ IT, či zamestnanec OINF zistí pokus o narušenie bezpečnosti IT týkajúce sa ochrany dát, je povinný takémuto pokusu podľa svojich schopností a možností zabrániť a okamžite o tom informovať svojho nadriadeného.

(11) V prípade prítomnosti zástupcu servisnej alebo dodávateľskej firmy je zodpovedný vedúci zamestnanec povinný určiť zamestnanca, ktorý bude zodpovedný za dohľad

nad dodržiavaním ustanovení tejto smernice zo strany zástupcu alebo zástupcov servisných alebo dodávateľských firiem.

(12) V prípade poruchy zariadenia IT, ktoré by mohlo obsahovať dáta, musí technik OINF pred odovzdaním tohto zariadenia do opravy odstrániť všetky možné médiá, na ktorých by sa dáta mohli nachádzať (pevné disky, CD, DVD média a pod.).

(13) Ak je poškodený pevný disk, technik OINF je povinný dať zástupcovi servisnej firmy podpísať čestné prehlásenie o mlčanlivosti, ktoré bude súčasťou zmluvy, prípadne objednávky.

(14) Bez predchádzajúceho písomného súhlasu OINF je zakázané poskytovať v akejkoľvek forme akékoľvek údaje, dáta, databázy či prehľady o informačných systémoch iným osobám, organizáciám.

(15) Zamestnanec OINF zabezpečí inštaláciu, prevádzku a priebežnú aktualizáciu antivírusového systému pre všetky PC, ktoré používajú zamestnanci prevádzkovateľa.

(16) Každý bezpečnostný incident, ktorý sa vyskytne na hardvéri, softvéri alebo zariadeniach počítačovej siete, musí byť okamžite ohlásený podľa jeho povahy buď správcovi siete, správcovi aplikácie, databázovému administrátorovi, systémovému administrátorovi. Dokumentáciu o všetkých bezpečnostných incidentoch, ktoré sa vyskytli sa vedú v denníku incidentov.

(17) OINF bez predchádzajúceho informovania príslušných vedúcich zamestnancov resp. službu konajúceho personálu nepoverí osobu ani firmu na vstup do priestorov. Akýkoľvek pokus o vstup s odvolaním na informačné technológie bez predchádzajúceho informovania zo strany OINF sa považuje za bezpečnostný incident.

(18) Pri podozrení na takúto skutočnosť je to zamestnanec povinný okamžite hlásiť ako pokus o bezpečnostný incident svojmu nadriadenému aj OINF.

(19) **Všeobecne platí, že všetko, čo nie je výslovne povolené – je zakázané!**

Článok X

PRÁCA S CITLIVÝMI A OSOBNÝMI DÁTAMI

(1) Všetci zamestnanci sú povinní manipulovať s dátami a dátovými nosičmi obsahujúcimi citlivé informácie o firemných aktivitách, odberateľoch, dodávateľoch, zamestnancoch, pacientoch a ďalších fyzických osobách tak, aby sa nedostali do rúk nepovolaných osôb. Porušenie tohto ustanovenia je závažným porušením pracovnej disciplíny a má za následok okamžité skončenie pracovného pomeru zamestnanca.

(2) Zásady spracúvania údajov sú základnými mantinelmi, v rámci ktorých sa konkrétne spracúvanie osobných údajov fyzickej a právnickej osoby posudzuje a vykonáva. Cieľom zásad spracúvania údajov je vykonávanie spracúvania údajov tak, aby boli rešpektované práva dotknutých osôb a aby spracúvaním údajov nedochádzalo k porušovaniu práva na zachovanie ľudskej dôstojnosti alebo k iným neoprávneným zásahom do práva na ochranu súkromia.

a) Zásada zákonnosti – osobné a citlivé údaje možno spracúvať len zákonným spôsobom a tak, aby nedošlo k porušeniu základných práv dotknutej osoby.
b) Zásada obmedzenia účelu – údaje sa môžu získavať len na konkrétne určený, výslovne uvedený a oprávnený účel a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmto účelom.
c) Zásada minimalizácie osobných údajov – spracúvané údaje musia byť primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú.
d) Zásada správnosti údaje spracúvané na určitý účel musia byť správne, presné a podľa potreby aktualizované tak, aby sa zabezpečilo, že sa údaje, ktoré sú nesprávne bezodkladne vymažú alebo opravia.
e) Zásada minimalizácie uchovávania – údaje musia byť uchovávané vo forme, kým je to potrebné na účel, na ktorý sa údaje spracúvajú.
f) Zásada integrity a dôvernosti – údaje musia byť spracúvané spôsobom, ktorý prostredníctvom primeraných technických a organizačných opatrení zaručuje primeranú bezpečnosť údajov vrátane ochrany pred neoprávneným a nezákonným spracúvaním údajov, náhodnou stratou, výmazom, alebo poškodením.
g) Zásada zodpovednosti – prevádzkovateľ je zodpovedný za dodržiavanie základných zásad spracúvania osobných údajov, za súlad spracúvania osobných

údajov so zásadami spracúvania osobných údajov a je povinný tento súlad so zásadami spracúvania osobných údajov na požiadanie úradu preukázať.

h) Cezhraničný prenos údajov do tretej krajiny, ktorá nezaručuje primeranú úroveň ochrany údajov, možno uskutočniť, ak dotknutá osoba pred jeho uskutočnením poskytla písomný súhlas s vedomím, že tretia krajina nezaručuje primeranú úroveň ochrany údajov. Súhlas musí obsahovať názov krajiny, do ktorej bude uskutočnený prenos údajov, ako aj upozornenie, že táto krajina nezaručuje primeranú úroveň ochrany údajov.

(3) Likvidácia osobných a citlivých údajov

a) Po skončení účelu spracovania údajov je potrebné tieto osobné údaje zlikvidovať, pokiaľ osobitný zákon nenariaďuje inak.

b) Dokumenty v listinnej podobe, obsahujúce osobné a citlivé údaje, možno uchovávať po dobu určenú na ich uchovanie, v zmysle registratúrneho poriadku prevádzkovateľa. Po ukončení doby uchovania je potrebné tieto dokumenty zlikvidovať.

c) Údaje, ktoré sú v IS spracúvané v elektronickej podobe, vrátane údajov na pamäťových médiách, ako napríklad pevné disky, USB kľúče, DVD, CD, veľkokapacitné externé pevné disky, sa uchovávajú v tejto podobe len na nevyhnutne potrebnú dobu, ktorá je určená účelom informačného systému. Po jej uplynutí sa bezpečným spôsobom likvidujú tak, aby údaje nebolo možné obnoviť.

d) Pamäťové médiá, vrátane diskov v serveroch a pracovných staniciach, ktoré boli použité na uloženie osobných a citlivých údajov v elektronickej podobe, musia byť pred svojim trvalým vyradením upravené tak, aby z nich nebolo možné obnoviť osobné údaje, ktoré na nich boli zapísané. Oddelenie informatiky, archívu a registratúry v koordinácii s príslušným odborom to zabezpečí prepísaním celého pamäťového média náhodnými údajmi alebo fyzickým zničením pamäťového média.

(4) Mlčanlivosť

a) Používateľ je povinný zachovávať mlčanlivosť o osobných a citlivých údajoch, ktoré spracúva.

b) Povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných a citlivých údajov.

c) Povinnosť mlčanlivosti neplatí, ak je to nevyhnutné, na plnenie úloh súdu a orgánov činných v trestnom konaní podľa osobitného zákona.

(5) Minimálne bezpečnostné zásady

a) získavať na základe svojho pracovného zaradenia len nevyhnutné údaje výlučne na vopred ustanovený účel

b) spracúvať jedine také údaje, ktoré sú nevyhnutne potrebné na dosiahnutie cieľa spracovania

c) spracúvať údaje len v priestoroch na to určených

d) o preprave osobných a citlivých údajov v písomnej forme alebo na pamäťových médiách mimo týchto priestorov môže rozhodnúť jedine príslušný vedúci zamestnanec; v takom prípade musí byť zabezpečená ochrana, dôvernosť, dostupnosť a integrita prepravovaných údajov

e) oznámiť príslušnému vedúcemu zamestnancovi a zodpovednej osobe každý bezpečnostný incident (napríklad podozrenie na únik osobných a citlivých údajov, neoprávnené zasahovanie do osobných a citlivých údajov) a oznámiť každé zistenie o nedostatočnej účinnosti existujúcich bezpečnostných opatrení prijatých na ochranu osobných a citlivých údajov

f) chrániť údaje v listinnej alebo elektronickej podobe pred stratou, poškodením, zneužitím, odcudzením, neoprávneným sprístupnením, poskytnutím, alebo inými neprípustnými formami spracúvania

g) umožniť vstup do miestnosti, v ktorej oprávnená osoba spracúva osobné a citlivé údaje neoprávneným osobám (napríklad upratujúci personál, servisní zamestnanci, návštevy...) až po zabezpečení ochrany údajov najmä uzatvorením dokumentov v elektronickej podobe, zatvorením spisového materiálu v listinnej podobe.

h) využiť všetky dostupné prostriedky na zabezpečenie údajov pred prístupom neoprávnenej osoby (napríklad uchovávanie dokumentov v uzamknutých častiach nábytku, uzamykanie miestnosti počas dočasnej neprítomnosti...)

i) používateľ je povinný dodržať ďalšie postupy upravené poučením, touto smernicou, iným vnútorným predpisom prevádzkovateľa, zákonom alebo iným všeobecne záväzným právnym predpisom.

j) Pokiaľ používateľ nebol poučený k spracúvaniu osobných a citlivých údajov pred začatím jeho spracovania alebo z poučenia iných vnútorných predpisov prevádzkovateľa jej nie je zrejmé, ako má plniť vyššie pomenované úlohy, je povinná o tejto skutočnosti informovať svojho nadriadeného a spracovanie údajov obmedziť len na úlohy, ktoré sú jej zrejmé.

k) Pri automatizovanom spracúvaní osobných a citlivých údajov používať programové vybavenie, ktoré vyžaduje meno a heslo používateľa.

l) Údaje, ktoré sa spracúvajú automatizovaným spôsobom je potrebné pravidelne zálohovať.

m) Údaje je v závislosti od ich citlivosti potrebné pseudonymizovať a šifrovať.

n) Na všetkých vstupoch do automatizovaného informačného systému je nevyhnutné používať antivírovú ochranu.

o) Priestory určené pre spracúvanie osobných a citlivých údajov musia byť zamknuté mimo pracovnej doby, aj pri dočasnej pracovnej neprítomnosti oprávnenej osoby.

p) Všetci zamestnanci musia byť poučený o povinnostiach súvisiacich s ochranou osobných a citlivých údajov.

q) Písomné dokumenty je potrebné archivovať v uzamykateľných skriniach.

r) Mať zaužívaný transparentný systém zaznamenávania bezpečnostných incidentov.

s) Zamestnanci musia nepotrebné elektronické dokumenty likvidovať zmazaním zo softvérového aj hardvérového zariadenia a písomné dokumenty likvidovať skartovaním.

PRÍLOHY

Príloha č. 1 Požiadavkový list na pridelenie prístupu k IS

OBOZNÁMENIE SA S IT SMERNICOU O KYBERNETICKEJ BEZPEČNOSTI FAKULTNEJ NEMOCNICE S POLIKLINIKU NOVÉ ZÁMKY

Prezenčná listina zo dňa:

Meno a priezvisko zamestnanca	Osobné číslo	Podpis

Hore uvedené osoby svojim podpisom prehlasujú, že Zamestnávateľ - Fakultná nemocnica s poliklinikou Nové Zámky, so sídlom Slovenská 2323/11 A, 94034 Nové Zámky, IČO: 17336112 ich oboznámil so „Smernicou o používaní informačných technológií FNsP Nové Zámky“, tejto porozumeli a budú ju pri výkone svojej činnosti rešpektovať.

ZMENOVÝ DENNÍK

Majiteľom procesu aktualizácie tohto dokumentu je: manažér kvality FNsP Nové Zámky.

Zmenu definitívne schvaľuje Rada riaditeľov FNsP.

Systémovú zodpovednosť za zmeny týkajúce sa tohto dokumentu/normy nesie: vedúci OINF.

Spracovateľ je zároveň správca dokumentu a je zodpovedný za jeho pravidelnú trojročnú revíziu.

Revízia 1: Dátum: Podpis:	Revízia 2: Dátum: Podpis:	Revízia 3: Dátum: Podpis:	Revízia 4: Dátum: Podpis:	Revízia 5: Dátum: Podpis:

Por. č. vydania	Dátum platnosti nového vydania	Poznámka (základný popis, dôvod zmeny, nového vydania)

ROZDEĽOVNÍK

ČÍSLO VÝTLAČKU	PRIDELENÉ		DÁTUM	PODPIS
	MENO A PRIEZVISKO	FUNKCIA		
1	JUDr. Lenka HORVÁTH BODÁKOVÁ	Právny referát		
2	Ing. Ladislav SLOBODA	vedúci Odboru informatiky		
3	Ing. Ladislav ČERI, PhD.	Manažér kvality		