FNsP F. D. Roosevelta
BANSKÁ BYSTRICA

| Dokument<br>**Riadený** | Účinnosť<br>**01.07.2025** | Určené<br>**Vlastníkom a správcom IT aktív a zamestnancom právneho oddelenia FNsP FDR BB** | Strana **1 z 6** |
|---|---|---|---|
| | Norma<br>**EN ISO 9001: 2015** | | Číslo vydania<br>**3** |

**Výtlačok č.**

Číslo dokumentu:

**S – A – 226**

**VYDANIE TRETIE**

Názov:

# INFORMAČNÁ A KYBERNETICKÁ BEZPEČNOSŤ – ŠPECIFIKÁCIA A ROZSAH BEZPEČNOSTNÝCH OPATRENÍ

Stupeň dôvernosti: **Interné**

Dátum vydania: 16.06.2025

**Predpis ruší:** S-A-225 IKB – Špecifikácia a rozsah bezpečnostných opatrení, vydanie 2, dátum vydania 03.07.2023

EVIDENCIA ZMIEN

| Číslo vydania | Číslo zmeny | Čísla menených listov | Účinnosť od / podpisy |
|---|---|---|---|
| | | | |
| | | | |

| | **Spracoval** | **Kontroloval** | **Schválil** |
|---|---|---|---|
| **Meno:** | Ing. Marta Adamjáková | Ing. Ivana Sklenková, MHA | Ing. Miriam Lapuníková, MBA |
| **Funkcia:** | manažér kybernetickej bezpečnosti | ekonomicko-prevádzková námestníčka | riaditeľka |
| **Podpis:** | | | |
| **Dátum:** | 06.06.2025 | 12.06.2025 | 16.06.2025 |

## OBSAH

# 1 ÚČEL

Účelom tohto dokumentu je určiť špecifikáciu a rozsah bezpečnostných opatrení a pravidlá pre vzťahy s dodávateľmi a partnermi a zabezpečiť ochranu aktív Fakultnej nemocnice s poliklinikou F. D. Roosevelta Banská Bystrica so sídlom Námestie L. Svobodu 1, Banská Bystrica, IČO: 00165549 (ďalej len „FNsP FDR BB“), ku ktorým pristupujú dodávatelia.

Tento vnútorný predpis zároveň určuje postupy na zabezpečenie informačnej a kybernetickej bezpečnosti.

# 2 ROZSAH PLATNOSTI

Tento dokument je aplikovaný na všetkých vlastníkov a správcov IT aktív, pre zamestnancov právneho oddelenia a pre všetkých zmluvných dodávateľov a partnerov, ktorí majú schopnosť ovplyvňovať dôvernosť, integritu a dostupnosť citlivých informácií vo FNsP FDR BB.

# 4 POJMY A SKRATKY

## 3.1 Pojmy

**Interný dokument** - citlivý dokument dostupný všetkým zamestnancom FNsP FDR BB.
**Chránený dokument** - citlivý dokument dostupný len určeným zamestnancom FNsP FDR BB.
**Správca IT aktíva** – zamestnanec, ktorý je zodpovedný za správu aktíva, jeho prevádzku a servis a má k tomu príslušné právomoci alebo oprávnenia od vlastníka IT aktíva.
**Vlastník IT aktíva** – zamestnanec, ktorý rozhoduje o používaní a rozvoji IT aktíva. Zabezpečuje jeho prevádzku a chod. Vlastník IT aktíva je zodpovedný za adekvátnu ochranu zvereného IT aktíva počas jeho celého životného cyklu.
**Vlastník zmluvy** - zamestnanec FNsP FDR BB, ktorý zastupuje FNsP FDR BB vo výkone jej práv a povinností vyplývajúcich zo zmluvy voči zmluvnému partnerovi.

## 3.2 Skratky

| | |
|---|---|
| FNsP FDR BB | Fakultná nemocnica s poliklinikou F. D .Roosevelta Banská Bystrica |
| IKB | Informačná a kybernetická bezpečnosť |
| MKB | Manažér kybernetickej bezpečnosti |

Pojmy a skratky použité v tomto dokumente sú popísané v dokumente S-A-208 Slovník termínov informačnej a kybernetickej bezpečnosti.

# 4 ZODPOVEDNOSTI A PRÁVOMOCI

1. Za spracovanie tohto dokumentu zodpovedá MKB, ktorý v ročných intervaloch preskúma aktuálnosť obsahu dokumentu a ak je to potrebné, zabezpečí aktualizované vydanie dokumentu. Z preskúmania vyhotoví záznam.

   MKB pri hodnotení účinnosti a primeranosti tohto dokumentu berie do úvahy nasledujúce kritériá:

   - počet a závažnosť incidentov vyplývajúcich z dodávateľských a partnerských činnosti;
   - počet zmlúv, kde vlastník zmluvy nie je definovaný.

2. S obsahom tohto dokumentu sa povinne oboznamujú vlastníci a správcovia IT aktív FNsP FDR BB, vlastníci zmlúv IT aktív a zamestnanci právneho oddelenia.

# 5 ŠPECIFIKÁCIA A ROZSAH BEZPEČNOSTNÝCH OPATRENÍ

## 5.1 Podmienky pre vytvorenie VPN prístupu

Pre zamestnancov dodávateľov môže byť vzdialený prístup vytvorený len za podmienky, že medzi týmto dodávateľom a FNsP FDR BB je uzatvorená platná zmluva vrátane ustanovení týkajúcich sa kybernetickej bezpečnosti.

Vzdialený prístup sa vytvára na základe žiadosti dodávateľa o zriadenie prístupu k IT aktívam FNsP FDR BB. Žiadosť o prístup pre konkrétnych zamestnancov dodávateľa odošle kontaktná osoba dodávateľa uvedená v zmluve na email security@nspbb.sk. V žiadosti sa dodávateľ musí zaviazať, že FNsP FDR BB oznámi každú skutočnosť, ktorá by mohla mať za následok zrušenie prístupu (napr., že pominuli dôvody zriadenia vzdialeného prístupu; že osoba, pre ktorú bol prístup zriadený už nie je zamestnancom dodávateľa; že dodávateľ ukončil zmluvný vzťah s FNsP FDR BB a iné).

Žiadosť dodávateľa schvaľuje vlastník IT aktíva, ku ktorému sa bude dodávateľ pripájať a vedúci Oddelenia IT.

Po schválení žiadosti správca IT aktíva, ktorým sa vytvára pripojenie z externého prostredia do interného prostredia, zriadi pre schválených zamestnancov dodávateľa bezpečné šifrované vzdialené prístupy.

## 5.2 Obmedzenia platné pre vytvorené VPN prístupy

Pre každý zriadený vzdialený prístup zamestnanca dodávateľa platia nasledovné obmedzenia:

- osobný certifikát sa vydáva s platnosťou najviac na 5 rokov,
- prístup je obmedzený len na konkrétne počítače resp. servery, ktoré boli uvedené v žiadosti,
- VPN prístup je overovaný službou Active Directory domény MS Windows.

## 5.3 Autentizácia

Platnosť autentizačných údajov (pre overenie osoby) pre zamestnancov dodávateľa je maximálne jeden rok, najdlhšie však do skončenia platnosti zmluvy. Kontaktná osoba dodávateľa musí pred uplynutím tejto doby podať žiadosť o predĺženie vzdialeného prístupu s uvedením dátumu trvania platnosti zmluvy. Správca IT aktíva, ktorým sa vytvára pripojenie z externého prostredia do interného prostredia, overí platnosť zmluvy a predĺži vzdialený prístup pre zamestnancov dodávateľa len ak je uzatvorená zmluva s dodávateľom stále platná a predĺženie schváli vedúci Oddelenia IT.

## 5.4 Zrušenie vzdialeného prístupu

Správca IT aktíva, ktorým sa vytvára pripojenie z externého prostredia do interného prostredia, zruší vzdialený prístup vždy ak:

- zistí, že sa vzdialený prístup nepoužíva na účely plnenia povinností dodávateľa,
- zistí bezpečnostný incident, ktorý vznikol v súvislosti s používaním vzdialeného prístupu,
- mu to nariadil vedúci oddelenia informačných technológií alebo MKB,
- užívateľ sa neprihlásil najmenej raz za 180 dní,
- dodávateľ ukončil zmluvný vzťah s FNsP FDR BB.

### 5.5 Povinnosti dodávateľa

Kontaktná osoba dodávateľa je povinná raz mesačne zaslať na email security@nspbb.sk informáciu o činnostiach, ktoré boli zo strany dodávateľa vykonané a to v minimálnom rozsahu dátum, časový rozsah vykonávanej činnosti, vykonaná činnosť, meno zamestnanca, ktorý činnosti vykonával. Forma a frekvencia hlásení môže byť, na základe žiadosti zaslanej kontaktnou osobou dodávateľa na email security@nspbb.sk, upravená po jej odsúhlasení vedúcim Oddelenia IT.

Kontaktná osoba dodávateľa je povinná na základe ustanovení zmluvy zabezpečiť vykonanie školenia vo vzťahu ku kybernetickej bezpečnosti a ustanoveniam zmluvy pre tých zamestnancov dodávateľa, ktorí pristupujú k IT aktívam FNsP FDR BB.

Kontaktná osoba dodávateľa je, na základe zmluvy, povinná zabezpečiť poučenie o povinnosti zachovávať mlčanlivosť pre tých zamestnancov dodávateľa, ktorí prichádzajú do styku s citlivými údajmi FNsP FDR BB.

### 5.6 Povinnosti zamestnancov dodávateľa so zriadeným vzdialeným prístupom

Zamestnancom dodávateľa sa:

- zakazuje zverejňovať alebo inej osobe vyzradiť svoje autentizačné údaje (používateľské meno a heslo);
- zakazuje držanie nezabezpečeného záznamu s autentizačnými údajmi (napr. na papieri, v softvérovom súbore, na prenosnom zariadení a pod.;
- zamestnanec je povinný chrániť pridelený autentizačný prostriedok pred odcudzením a zničením a nesmie ho prenechať inej osobe;
- zamestnanec je povinný všetky kryptografické kľúče (najmä privátne) chrániť pred odcudzením a zničením a nesmie ich prenechať inej osobe;
- zamestnanec je povinný pri strate, poškodení alebo inom narušení bezpečnosti kryptografických kľúčov alebo certifikátov bezodkladne zaslať informáciu o incidente na email security@nspbb.sk;
- zakazuje pristupovať k IT aktívam, ktoré nie sú predmetom zmluvného vzťahu a vykonávať na nich akúkoľvek činnosť;
- zakazuje na zverených IT aktívach vykonávať činnosti, ktoré nie sú predmetom zmluvného vzťahu.

## 6. ZMENOVÉ KONANIE

### 6.1 Evidencia zmien

| Poradové číslo vydania | Dátum platnosti nového vydania | Rozsah zmien |
|---|---|---|
| 1. | 01.11.2021 | Prvé vydanie |
| 2. | 10.07.2023 | Článok 7.2 Externé (Súvisiace predpisy) upravený zdroj vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., zrušený „§ 7 odsek h) vykonania poučenia o manipulácií s informáciami“. |

| Poradové číslo vydania | Dátum platnosti nového vydania | Rozsah zmien |
|---|---|---|
| 3. | 01.07.2025 | Aktualizácia v celom rozsahu – obsah smernice je upravený tak, aby obsahoval všetky potrebné informácie pre dodávateľov, pretože bude jedinou prílohou k zmluvám |

### 6.2 Zodpovednosti

Za kontrolu a aktuálny obsah smernice zodpovedá manažér kybernetickej bezpečnosti. Zmeny smernice sa vykonávajú podľa 1.SMK.DOK Riadenie dokumentácie a záznamov. Smernicu a jej zmeny schvaľuje štatutárny orgán FNsP FDR.

## 7. SÚVISIACE PREDPISY

### 7.1 Interné

### 7.2 Externé

1. Zákon NR SR č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
2. Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.
3. ISO/IEC 27001 štandard, články A.7.1.1, A.7.1.2, A.7.2.2, A.8.1.4, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2

## 8 PRÍLOHY

Bez príloh