NEMOCNICE HAVLÍČKŮV BROD
Husova 2624,
580 22 Havlíčkův Brod

BEZPEČNOSTNÍ STANDARD PRO DODAVATELE ICT A ZDRAVOTECHNIKY (BESDIZ)

Obsah: 3

1 ÚVOD

V souvislosti s plněním smluvních vztahů a zajištěním ochrany informačních aktiv **Nemocnice Havlíčkův Brod, příspěvkové organizace** (dále jen „NHB“) jsou pracovníci dodavatelů povinni seznámit se s níže uvedenými pravidly a řídit se jimi při veškeré pracovní činnosti vykonávané pro NHB.

Tento dokument stanovuje základní bezpečnostní požadavky a pravidla pro pracovníky dodavatelů, kteří vykonávají činnost v prostředí NHB nebo s jejími prostředky, a to v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, i ve znění pozdějších předpisů, a dále v souladu s vnitřními předpisy NHB v oblasti ochrany informací, bezpečnosti ICT a zdravotechniky.

2 POVINNOSTI PRACOVNÍKŮ DODAVATELE

Pracovník dodavatele je povinen být prokazatelně seznámen s podmínkami smlouvy, na jejímž základě vykonává pracovní činnost pro NHB, a tyto podmínky dodržovat. Zároveň se zavazuje respektovat následující pravidla týkající se výkonu činností:

- v prostorách NHB s využitím prostředků dodavatele;
- v prostorách NHB s využitím prostředků NHB;
- mimo prostory NHB s využitím prostředků NHB;
- mimo prostory NHB s využitím prostředků dodavatele.

Při všech činnostech musí pracovník dodavatele dodržovat stanovené i doporučené pracovní postupy a metodiky tak, aby nedošlo k narušení kybernetické bezpečnosti ani bezpečnosti informací zpracovávaných v rámci činností pro NHB.

Jakékoliv výjimky z těchto pravidel podléhají předchozímu schválení odpovědné osoby NHB a musí být ze strany dodavatele řádně evidovány. Odpovědnou osobou na straně NHB je možné kontaktovat na adrese **kb@onhb.cz**

Dodavatel je povinen oznámit svůj požadavek na zahájení prací s dostatečným předstihem, a to minimálně 7 kalendářních dnů před plánovaným zahájením, odpovědné osobě na straně NHB.

3 POHYB PRACOVNÍKŮ DODAVATELE V AREÁLU

Vzhledem ke specifickému charakteru provozu zdravotnického zařízení NHB a s ohledem na ochranu pacientských údajů, bezpečnost osob a provozní režim jednotlivých pracovišť, platí pro pracovníky dodavatelů následující pravidla týkající se pohybu v prostorách.

- Pracovník dodavatele má oprávnění vstupovat **pouze do prostor**, které jsou **nezbytné pro výkon sjednané činnosti**.
- Vstup do **režimových, klinických nebo jinak chráněných prostor** je možný **pouze se souhlasem a za přítomnosti pověřeného pracovníka NHB.**
- Pracovník dodavatele je povinen respektovat **všechna místní provozní, hygienická a bezpečnostní opatření**, která se vztahují na dané pracoviště.

- Pořizování obrazových, zvukových nebo jiných záznamů v prostorách NHB je pracovníkům dodavatele povoleno pouze po předchozím výslovném souhlasu odpovědné osoby NHB a výhradně za účelem dokumentace činností souvisejících s plněním smluvního vztahu.
- V případě nutnosti pohybu po areálu je dodavatel povinen zajistit, aby se pracovníci prokazatelně identifikovali a jednali v souladu s pokyny odpovědných osob.

4 POŽADAVKY NA ZAŘÍZENÍ PŘIPOJOVANÁ DO SÍTĚ

Do prostředí NHB lze připojovat pouze předem schválená zařízení, a to jak při fyzickém připojení do místní sítě (LAN), tak při vzdáleném přístupu prostřednictvím VPN.

Schválená zařízení musí splňovat následující požadavky

Technické požadavky

- Veškerý nainstalovaný software je **legální** a odpovídá **licenčním podmínkám** výrobce.
- Operační systém zařízení musí mít **platnou servisní podporu výrobce** (zejména v oblasti bezpečnostních aktualizací).

V případě, že to charakter zařízení umožňuje:

- **Automatické aktualizace** bezpečnostních záplat pro všechny klíčové komponenty (např. operační systém, kancelářské balíky, Java, databázové nástroje apod.) jsou **funkční a pravidelně prováděné**.
- Zařízení je vybaveno **funkčním a pravidelně aktualizovaným antivirovým programem** se zapnutým **rezidentním štítem**.
- Po vložení výměnných médií (např. USB disk, CD/DVD) je automaticky spouštěna **antivirová kontrola**.
- Na zařízení musí být aktivní **osobní firewall**, jehož pravidla jsou nastavena pouze na nezbytnou komunikaci v rámci plnění činností pro NHB.

Provozní podmínky

- Všechna zařízení připojovaná do sítě **musí mít předem předanou komunikační matici** zařízení odsouhlasenou odpovědnou osobou na straně NHB.
- Zařízení musí být připojeno **výhradně na místě definovaném NHB**, v souladu s provozními a bezpečnostními pravidly nemocnice.
- Zařízení **připojené do vnitřní sítě NHB nesmí být současně připojeno k internetu jinou cestou**.

5 PŘIDĚLOVÁNÍ OPRÁVNĚNÍ

Přidělování oprávnění pro přístup do ICT prostředí **NHB pracovníkům dodavatele** se řídí zásadou **nezbytného minima** (tzv. *need-to-know* princip). Přístupová oprávnění jsou personofikovaná, nejsou

náročová a jsou poskytována výhradně na základě odůvodněné potřeby vyplývající z předmětu smluvního vztahu.

Pracovník dodavatele **nesmí sdílet přístupové údaje, autentizační prostředky ani jiné identifikační informace** pro přístup do prostředí NHB s žádnou jinou osobou. V případě zjištění sdílení odpovídá za tento bezpečnostní incident osoba, která o přístup nebo výjimku požádala, a to na straně dodavatele.

Veškerá přístupová oprávnění smějí být využívána **výhradně k účelům plnění předmětu smlouvy**, a to v rozsahu a čase nezbytně nutném pro realizaci sjednaných činností.

Pokud je v rámci plnění smlouvy nezbytné poskytnutí **privilegovaných přístupových oprávnění** (např. administrátorských), jejich použití musí být:

- omezeno výhradně na úkony, které vyžadují danou úroveň oprávnění,
- časově omezené na dobu nezbytně nutnou,
- v žádném případě nesmí být privilegovaná oprávnění využívána pro běžné nebo rutinní úkony.

Pracovník dodavatele, kterému byl přidělen uživatelský účet, **nese plnou odpovědnost** za veškeré akce provedené pod tímto účtem v prostředí NHB.

6 POLITIKA HESEL

V rámci přístupu do informačních systémů NHB je pracovník dodavatele povinen dodržovat níže uvedená pravidla pro tvorbu, správu a ochranu autentizačních údajů.

Požadavky na tvorbu hesel

- **Minimální délka hesla:**
    - běžný uživatel: **min. 12 znaků**,
    - administrátor nebo privilegovaný účet: **min. 17 znaků**
    - Technický účet **min. 22 znaků**
- **Kombinace znaků:**
    - Heslo musí obsahovat **alespoň 3 z následujících 4 typů znaků**:
    - malá písmena (a–z),
    - velká písmena (A–Z),
    - číslice (0–9),
    - speciální znaky (např. !, @, #, %, apod.).

Zakázané prvky v heslech

- **Heslo nesmí** obsahovat:
    - běžně používaná nebo snadno odhadnutelná hesla (např. "123456", "password"),
    - přihlašovací jméno, e-mail uživatele, název systému nebo jiné zjevné souvislosti,
    - opakující se nebo sekvenční znaky (např. "aaaa", "abc123"),
    - jména, příjmení nebo data narození uživatele, jeho rodinných příslušníků či přátel,
    - části obsahující aktuální rok, měsíc, sezónu (např. "Summer2025", "leden2024").

Správa hesel

- **Hesla nesmí** být zaznamenána v čitelné podobě, a to ani písemně, ani elektronicky (např. v souborech, e-mailech, poznámkách apod.).
- V případě prozrazení hesla je uživatel **povinen heslo okamžitě změnit** a neprodleně informovat odpovědnou osobu NHB.
- Všechny bezpečnostní incidenty spojené s únikem nebo zneužitím přihlašovacích údajů musí být bezodkladně ohlášeny.

7 INSTALACE SOFTWARE

Instalace jakéhokoliv softwaru do informačního prostředí NHB je možná pouze na základě předchozího schválení ze strany odpovědného pracovníka NHB.

Instalační postupy, použité softwarové balíky i související konfigurace musí být předem konzultovány a odsouhlaseny odpovědnou osobou na straně NHB. Bez tohoto souhlasu není instalace žádného softwaru povolena, a to ani v případě, že se jedná o běžně dostupný nebo bezplatný software.

Toto pravidlo platí pro:

- nové instalace na zařízeních NHB,
- dočasné instalace pro účely servisu, testování či podpory,

8 VÝVOJ A ÚDRŽBA

Veškeré činnosti spojené s vývojem, úpravami nebo údržbou systémů, aplikací či infrastrukturních prvků v prostředí **NHB** musí být realizovány v souladu s následujícími zásadami.

Schvalování a plánování

- **Jakékoli vývojové nebo servisní zásahy** (včetně změn konfigurace, aktualizací, skriptů, automatizací nebo migrací) **musí být prokazatelně předem schváleny odpovědným pracovníkem NHB**.
- Všechny změny musí být **dokumentovány**, včetně účelu, rozsahu, technického popisu a odpovědné osoby.
- V případě zásahu do produkčního prostředí musí být předem vyhodnocen **dopad na provoz nemocnice** a provedení změn musí být koordinováno tak, aby **nedocházelo k omezení nebo ohrožení poskytování zdravotní péče**.

Realizace změn

- Změny a údržba musí být prováděny **v souladu s kapitolou řízení změn.**
- Veškeré zásahy do systémů musí být **dohledatelné** – prostřednictvím logování, verzování a průkazné evidence.
- U změn, které mohou ovlivnit funkčnost, bezpečnost nebo výkon systémů, je povinné provést **testování v neprodukčním prostředí** před nasazením do provozu a zajištění možnosti "rollbacku" na funkční ověřenou verzi.

Dodavatel je povinen poskytnout NHB veškerou dokumentaci k provedeným změnám a zajištění jejich zpětné dohledatelnosti (např. logy, konfigurace, revize kódu).

9 ŘÍZENÍ ZMĚN

Veškeré změny realizované v prostředí **NHB** v rámci dodávky služeb či plnění smluvních závazků podléhají řízenému procesu. Změny se dělí na **významné** a **nevýznamné**. Každou plánovanou změnu je dodavatel povinen předem oznámit odpovědné osobě NHB. **Významné změny** musí být schváleny před jejich realizací.

Významná změna je taková, která:

- ovlivňuje bezpečnost kritických dat a systémů,
- zahrnuje centrální ICT aktiva, zdravotechniku anebo primární aktiva nemocnice,
- má složitý a časově náročný postup pro navrácení do původního stavu,
- vyžaduje účast více pracovníků nebo externí podpory pro její provedení,
- způsobí odstávku delší než 12 hodin a zároveň ovlivňuje provoz organizačních jednotek během hlavního provozního času.

Nevýznamná změna je taková, která:

- se nijak nedotýká bezpečnosti kritických dat a systémů,
- ovlivňuje pouze omezenou část infrastruktury nebo jednotlivé oddělení,
- má snadný a rychlý postup navrácení do původního stavu,
- je proveditelná jednotlivcem nebo běžnou IT podporou,
- způsobí odstávku kratší než 12 hodin, která nemá dopad na provoz v hlavním čase.

Postup pro realizaci změn:

- Významné změny musí být předem písemně schváleny odpovědnou osobou NHB a mít zpracovaný plán změny, včetně testování a způsobu návratu do původního stavu.
- Nevýznamné změny mohou být prováděny operativně, avšak vždy musí být evidovány a dohledatelné.
- Veškeré změny musí být zdokumentovány, včetně data provedení, odpovědné osoby a případných dopadů.
- NHB si vyhrazuje právo kdykoliv vyžádat dodatečné informace nebo úpravy plánované změny.

10 VÝMĚNNÁ MÉDIA

V prostředí NHB je používání výměnných paměťových médií (např. USB flash disky, externí pevné disky apod.) striktně omezeno a podléhá následujícím pravidlům:

- Používat lze výhradně registrovaná a schválená média, která jsou evidována a spravována NHB nebo jsou majetkem NHB.
- Pokud pracovník dodavatele potřebuje výměnné médium ke své činnosti, bude mu zapůjčeno na nezbytně nutnou dobu pověřeným pracovníkem NHB.

Na zapůjčeném médiu mohou být ukládána pouze data a informace přímo související s plněním smluvního díla, a to pouze v rozsahu nezbytném pro konkrétní úkon (např. přenos dat mezi systémy NHB).

Omezení a pravidla použití

- Data smějí být na výměnném médiu uchovávána jen po dobu nezbytně nutnou k přenosu nebo zpracování.
- Výměnná média nesmějí být používána pro zálohování dat ani pro dlouhodobé uchovávání jakýchkoli informací.
- Před každým použitím výměnného média musí být provedena antivirová kontrola.
- médium nesmí být použito na jiných zařízeních mimo prostředí NHB bez předchozího schválení.

Výše uvedené se se nevztahuje na instalační/aktivační média, která jsou nedílnou součástí dodávky a nelze je nahradit nebo přemístit na jiný disk

11 ZAKÁZANÉ ČINNOSTI

V NHB je pracovníkům dodavatele výslovně zakázáno provádět následující činnosti:

Obecně zakázané aktivity

- Provádět bez předchozího schválení odpovědnou osobou NHB jakékoli úpravy nebo zásahy do komunikační infrastruktury nemocnice, zejména do síťových prvků, kabeláže a aktivních zařízení (např. switche, směrovače apod.).
- Ukládat, sdílet nebo jinak zpracovávat data a informace eticky nevhodného obsahu, odporující dobrým mravům, zákonům nebo poškozující dobré jméno NHB.
- Stahovat, ukládat, šířit nebo instalovat jakýkoliv obsah (zejména datové a spustitelné soubory) v rozporu s platnými licenčními podmínkami nebo zákony o ochraně duševního vlastnictví.
- Navštěvovat webové stránky s nevhodným, neetickým, nezákonným nebo rušivým obsahem, zejména stránky s obsahem erotickým, extremistickým nebo propagujícím násilí.
- Šířit spam nebo jiný nevyžádaný digitální obsah, včetně pokusů o phishing nebo sociální inženýrství.
- Pokoušet se o jakýkoliv neautorizovaný přístup do informačních systémů, aplikací nebo zařízení NHB.

Zakázané nástroje a programy

Instalace, spouštění nebo používání následujících nástrojů je v prostředí NHB striktně zakázána, pokud nejsou výslovně schváleny jako součást předmětu plnění:

- **Keyloggery** – software nebo hardware určený k zaznamenávání stisků kláves, narušující důvěrnost zadávaných dat.
- **Sniffery** – nástroje pro zachytávání síťového provozu, které mohou vést k úniku dat nebo porušení soukromí.
- **Analyzátory zranitelností** – nástroje určené k vyhledávání slabin v systémech, portech a síťových službách bez výslovného schválení.
- **Backdoory** – skryté prostředky pro obcházení autentizačních mechanismů za účelem budoucího neautorizovaného přístupu.
- **Malware** a jakýkoli jiný software, který obchází, narušuje nebo omezuje bezpečnostní opatření NHB.
- **Obdobné rizikové nebo útočné nástroje**, jejichž cílem je narušení důvěrnosti, dostupnosti, integrity nebo neautorizovaný přístup k datům.

12 HLÁŠENÍ BEZPEČNOSTNÍCH UDÁLOSTÍ A INCIDENTŮ

Dodavatel je povinen bez zbytečného prodlení oznámit odpovědným pracovníkům NHB jakékoliv podezření na kybernetickou bezpečnostní událost či incident. Zároveň je povinen poskytnout nezbytnou součinnost, včetně poskytnutí relevantních informací a dat potřebných pro vyšetření, analýzu a následná nápravná opatření.

Definice

- **Kybernetická bezpečnostní událost (KB událost)**
  Událost, která může mít za následek narušení bezpečnosti informací v informačních systémech, narušení poskytovaných služeb, nebo ohrožení bezpečnosti a integrity elektronických komunikačních sítí. Jde o situaci, která má potenciál stát se kybernetickým bezpečnostním incidentem.
- **Kybernetický bezpečnostní incident (KB incident)**
  Událost, u které došlo ke skutečnému narušení bezpečnosti informací, služeb nebo sítí. Jde o porušení důvěrnosti, integrity nebo dostupnosti dat, případně o narušení dostupnosti nebo interoperability poskytovaných služeb a elektronických komunikačních sítí.

Povinnosti dodavatele

- Aktivně sledovat a vyhodnocovat chování systémů a zařízení, která jsou využívána při plnění smluvních závazků vůči NHB.
- Bezodkladně hlásit jakýkoliv výskyt nebo podezření na KB událost/incident.
- Spolupracovat při šetření události/incidentu na vyžádání NHB nebo jejích pověřených pracovníků.
- Zdržet se jakéhokoliv zakrývání, oddalování nebo zatajování informací týkajících se KB incidentů.

13 MONITORING ČINNOSTÍ

Veškeré přístupy a aktivity pracovníků dodavatele vztahující se k informačním aktivům a infrastruktuře NHB jsou nepřetržitě zaznamenávány, monitorovány a vyhodnocovány s cílem zajistit kybernetickou a provozní bezpečnost.

Pracovník dodavatele bere na vědomí, že jeho činnost v prostředí NHB podléhá dohledu, a to v rozsahu nezbytném pro:

- ochranu důvěrnosti, integrity a dostupnosti informačních systémů a dat,
- prevenci, detekci a analýzu bezpečnostních hrozeb,
- dodržení zákonných a smluvních povinností NHB.

V případě zjištění podezřelého, závadného nebo nestandardního chování může být:

- přístupový účet pracovníka dočasně zablokován,
- aktivován proces zvládání bezpečnostních incidentů podle interních postupů NHB,
- případ dále analyzován ve spolupráci s dodavatelem a odpovědnými osobami NHB.

14 ZÁVĚREČNÉ USTANOVENÍ

Porušení zde uvedených pravidel, zásad a povinností může být ze strany **NHB** považováno za **závažné porušení smluvních podmínek**, které může vést k:

- **okamžitému přerušení spolupráce**,
- **omezení přístupových práv**,
- **uplatnění sankcí** dle smlouvy nebo právních předpisů,
- a v odůvodněných případech také k **oznámení bezpečnostního incidentu** příslušným dozorovým orgánům nebo k zahájení právních kroků.

NHB si vyhrazuje právo tento dokument aktualizovat v souladu s platnou legislativou, vývojem bezpečnostních standardů a provozními potřebami nemocnice. O změnách bude dodavatel informován před jejich účinností.