NEMOCNICE PRACHATICE a.s.

Bezpečnostní pravidla pro běžné dodavatele

(dle zákona č. 264/2025 sb., o kybernetické bezpečnosti a souvisejících zákonech a vyhláškách)

Obsah

Platné od: 1.3.2026
Verze: 1.1

Seznam zkratek a pojmů

IT	Informační technologie
ISMS	Systém řízení bezpečnosti informací
NDA	Dohoda o mlčenlivosti
ICT	Informační a komunikační technologie
OS	Operační systém
MFA	Vícefaktorová autentizace

1. Úvod

Bezpečnostní pravidla stanovená v tomto dokumentu jsou obecně platná pro všechny dodavatele, servisní organizace, poskytovatele ICT služeb, konzultanty, vývojáře, výzkumné organizace, poskytovatele cloudových řešení, obchodní partnery a další smluvní partnery **Nemocnice Prachatice, a.s.**, dále uváděné pod souhrnným označením „Externí subjekt“, kteří mají na základě vzájemných pracovně právních nebo jiných smluvních vztahů oprávnění přistupovat zevnitř nebo zvenčí k počítačové síti, datům nebo technickým a klinickým prostorám a zpracovávaným informacím v jakékoliv podobě a formě.

1.1. Cíle

Základním cílem systému řízení bezpečnosti informací v Nemocnici Prachatice, a.s. je zajištění dostupnosti informačních aktiv jen oprávněným osobám, správnosti a kompletnosti informací, důvěrnosti a bezpečnosti jejich zpracování a ochrany informací proti náhodnému nebo neoprávněnému zničení nebo náhodné ztrátě, proti neoprávněnému přístupu, změnám nebo šíření, a to v souladu se zákony a jinými právními předpisy ČR.

1.2. Principy

Nezbytnou prioritou při práci s informacemi v jakékoliv podobě je zajistit, aby veškeré zpracovávané informace byly trvale spolehlivé, správné, důvěryhodné a náležitě chráněné před relevantními hrozbami. Z tohoto důvodu jsou implementována odpovídající bezpečnostní opatření, jejichž účelem je naplňovat základní bezpečnostní principy:

- Důvěrnost – zajištění toho, aby k informacím měly přístup výhradně autorizované osoby disponující odpovídajícími oprávněními.
- Integrita – zajištění správnosti, úplnosti a neporušenosti informací, datových toků a souvisejících procesů.
- Dostupnost – zajištění, že oprávnění uživatelé mají přístup k informacím v okamžiku, kdy je jejich využití nezbytné nebo oprávněně požadované.

1.3. Rozsah a působnost

Tato bezpečnostní pravidla se vztahují na veškeré činnosti, procesy, aktiva a subjekty, které se podílejí na zpracování, uchovávání, přenosu nebo ochraně informací v rámci Nemocnice Prachatice, a.s.

Bezpečnostní pravidla se konkrétně vztahují na:

- informační aktiva – veškeré informace v digitální i fyzické podobě, jejichž vlastníkem nebo správcem je Nemocnice Prachatice, a.s., včetně osobních, citlivých, provozních a finančních údajů,
- všechny organizační, provozní a technické procesy, které pracují s informacemi
- veškeré systémy, aplikace a datová úložiště,
- zařízení, infrastrukturu a sítě, ke kterým externí subjekty získávají přístup,
- dodávky a provoz softwarových i hardwarových řešení.

2. Organizační opatření

Externí subjekty, požadující přístup k informacím a informačním systémům Nemocnice Prachatice, a.s., musí splnit všechny relevantní níže uvedené bezpečnostní opatření.

2.1. Řízení bezpečnosti a odpovědnosti

Externí subjekt je povinen zajistit následující:

a) určit odpovědnou osobu, která zajišťuje komunikaci s organizací,
b) zajistit, že jejich pracovníci byli poučeni o základních pravidlech kybernetické bezpečnosti formou vstupních a průběžných školení,
c) provádět činnosti pouze osobami, které jsou k tomu určené a kompetentní,
d) oznamovat změny osob, které mají přístup, bez zbytečného odkladu.

2.2. Požadavky ve smluvních vztazích s externími dodavateli

Externí subjekt může získat přístup pouze na základě:

a) platné smlouvy nebo objednávky,
b) předem schváleného rozsahu přístupu,
c) povinnosti mlčenlivosti (NDA).

Smluvní dokumentace obsahuje:

a) popis poskytované služby,
b) vymezení povolených osob,
c) podmínky přístupu a způsob jeho schválení,
d) závazek dodržovat tato bezpečnostní pravidla.

2.3. Kategorie dodavatelů

Nemocnice Prachatice, a.s. stanovuje minimální bezpečnostní požadavky pro externí subjekty v závislosti na zařazení subjektu do některé z následujících kategorií:

Kategorie	**Popis**
Běžný dodavatel *ICT systémů*	Pro řízení dodavatele stačí méně náročná pravidla řízení dodavatelů, která jsou shodná pro všechny – zpravidla tzv. „Režim nižších povinností“ bez přístupu, nebo s mimořádným jednorázovým částečným přístupem k primárním aktivům a pouze s omezeným přístupem k podpůrným aktivům.
Významný dodavatel *ICT systémů*	K řízení dodavatele je potřeba zavést další bezpečnostní opatření nad rámec standardních pravidel – zpravidla tzv. „Režim vyšších povinností“.

2.4. Personální opatření

Externí subjekty, které v rámci smluvního vztahu získávají přístup k informačním systémům nebo informacím Nemocnice Prachatice, a.s., jsou povinny zajistit, aby všechny osoby podílející se na poskytování služeb splňovaly požadavky těchto bezpečnostních pravidel a souvisejících interních předpisů. Externí subjekty nesou plnou odpovědnost za jednání svých zaměstnanců či subdodavatelů ve vztahu k bezpečnosti informací.

2.4.1. Prověřování osob

Externí subjekt je povinen zajistit, aby osoby, které budou mít přístup k informačnímu systému nebo informacím Nemocnice Prachatice, a.s., byly před zahájením činnosti prověřeny v rozsahu odpovídajícím charakteru vykonávané práce. Prověřování musí zahrnovat zejména ověření identity, trestní bezúhonnosti tam, kde to povaha činnosti vyžaduje, a odborné způsobilosti. Externí subjekt je odpovědný za to, že na činnost související s provozem systémů nebo manipulací s daty Nemocnice Prachatice, a.s. budou nasazeny pouze kompetentní a řádně poučené osoby.

2.4.2. Školení v oblasti kybernetické bezpečnosti

Externí subjekt musí zajistit, aby jeho pracovníci disponovali přiměřenými znalostmi potřebnými pro bezpečné nakládání s informačními aktivy. Každý pracovník externího subjektu, který získá přístup, musí být před zahájením činnosti proškolen v oblasti kybernetické bezpečnosti a následně být pravidelně poučen o zásadách bezpečného chování. O příslušném školení je externím subjektem vedena evidence.

2.4.3. Pravidla přidělování a využívání přístupů

a) přístup je povolen pouze na nezbytně nutnou dobu,
b) přístupová práva odpovídají principu minimálních oprávnění,
c) přístupy jsou přidělovány po schválení vlastníka aktiva.

Externí subjekty jsou povinny:

a) používat vícefaktorové ověřování,
b) používat bezpečná zařízení (aktualizovaný OS, funkční a aktualizovaný antivirová ochrana, šifrování),
c) dodržovat pravidla pro vzdálený přístup,
d) zamezit přístupům třetích stran či subdodavatelů bez schválení.

2.4.4. Chování externích pracovníků na pracovištích poskytovatele

Osoby externího subjektu jsou povinny řídit se pravidly chování platnými pro zaměstnance Nemocnice Prachatice, a.s., zejména při pohybu v prostorách, manipulaci s technikou či citlivými informacemi. Pracovníci externích subjektů nesmí bez výslovného schválení provádět žádné činnosti, které mohou ovlivnit bezpečnost informačního systému a nesmí obcházet nastavená bezpečnostní opatření.

2.4.5. Ukončení spolupráce a odebrání přístupů

Externí subjekt je povinen oznámit ukončení pracovní činnosti nebo změnu role kteréhokoli svého pracovníka, jenž má přístup k informačním systémům poskytovatele, a to nejpozději v den vzniku této změny. Nemocnice Prachatice, a.s. po obdržení oznámení zajistí neprodlené odebrání přístupů, rušení účtů nebo úpravu oprávnění.

Externí subjekt je povinen zajistit:

- bezpečně předat veškerá data,
- odstranit kopie dat,
- vrátit zapůjčená zařízení,
- potvrdit likvidaci dat, pokud to stanovuje smlouva,
- ukončit veškeré přístupy do systémů,

2.4.6. Odpovědnost externího subjektu

Externí subjekt nese plnou odpovědnost za jednání svých zaměstnanců a osob jednajících jeho jménem. Porušení těchto bezpečnostních pravidel stanovených v tomto dokumentu může být posuzováno jako porušení smluvních závazků a může vést ke smluvním sankcím či k ukončení spolupráce.

2.5.Povinnosti externích subjektů během spolupráce

1) Aktivně chránit aktiva Nemocnice Prachatice, a.s., která mu byla svěřena.
2) Pravidelně informovat o změnách, které mohou mít dopad na bezpečnost.
3) Spolupracovat při řešení incidentů a poskytovat potřebné podklady.
4) Nepoužívat subdodavatele bez předchozího schválení Nemocnice Prachatice, a.s.
5) Zajistit proškolení svých zaměstnanců v oblasti ochrany informací.

2.6.Kontroly, audity a bezpečnostní dohled

Nemocnice Prachatice, a.s. může provádět:

a) pravidelné hodnocení dodržování bezpečnostních požadavků,
b) průběžné posuzování rizik souvisejících s daným externím subjektem související s dodávkou nebo poskytovanou službou.

Při nedodržení požadavků může Nemocnice Prachatice, a.s.:

a) vyžadovat nápravná opatření v definované lhůtě,
b) omezit nebo pozastavit přístupy,
c) ukončit smluvní vztah.

3. Technická opatření

3.1. Správa identit a autentizace

Každý uživatel musí mít jednoznačně identifikovatelnou identitu, která je vázána na jeho roli a odpovědnosti. Přístupy se přidělují podle principu minimálních oprávnění a jsou pravidelně přezkoumávány.

Externí uživatelé a třetí strany musí využívat zabezpečené autentizační mechanismy, které zahrnují silné heslo (minimálně 12 znaků u běžných účtů, minimálně 17 znaků u privilegovaných účtů a 22 znaků u technologických účtů, kombinace velkých a malých písmen, číslic a speciálních znaků) a všude, kde je to možné, vícefaktorovou autentizaci (MFA). Hesla musí být pravidelně měněna a nesmí být sdílena mezi uživateli ani ukládána v nezašifrované podobě. Administrátoři mají právo přidělovat oprávnění pouze po schválení odpovědné osoby.

3.2. Řízení přístupu

Pro účely přidělení přístupových práv externím subjektům jsou stanovena následující pravidla:

a) přístup je povolen pouze na nezbytně nutnou dobu,
b) přístupová práva odpovídají principu minimálních oprávnění,
c) přístupy jsou přidělovány na základě schválení Nemocnice Prachatice, a.s.

Externí subjekty jsou povinny:

a) používat více faktorové ověřování, kde to povaha služby vyžaduje,
b) používat bezpečná zařízení (aktualizovaný OS, antivir, šifrování),
c) oddělovat firemní zařízení od soukromých,
d) využívat šifrovanou komunikaci,
e) zamezit přístupům třetích stran či subdodavatelů bez schválení.

3.3.Zálohování dat

Externí subjekty musí zajistit, aby:

a) byla zálohována data, která spravuje v rámci poskytované služby, pokud je zálohování její součástí,
b) zálohy byly chráněny před zneužitím,
c) citlivá data nebyla ukládána mimo stanovená úložiště.

4. Fyzická bezpečnost

Nemocnice Prachatice, a.s. uplatňuje opatření k ochraně fyzických prostor a technických zařízení před neoprávněným přístupem. Externí subjekty jsou povinny tato opatření respektovat a dodržovat při jakémkoli vstupu do prostor Nemocnice Prachatice, a.s. nebo při manipulaci s jejími zařízeními.

4.1.Požadavky na přístup do prostor Nemocnice Prachatice, a.s.

Externí subjekty musí dodržovat následující pravidla:

a) Přístup do prostor Nemocnice Prachatice, a.s. je umožněn pouze na základě předem schválené a evidované návštěvy.
b) Všechny osoby z řad dodavatelů musí použít přidělené identifikační prostředky (návštěvní průkazy, přístupové karty).
c) Externí pracovníci mohou vstupovat pouze do prostor, které jsou nezbytné pro výkon jejich činnosti.
d) V kritických a citlivých oblastech Nemocnice Prachatice, a.s. mohou pracovat pouze v doprovodu pověřené osoby.
e) Externí pracovníci jsou povinni řídit se pokyny pověřeného pracovníka Nemocnice Prachatice, a.s. a nesmí umožnit vstup třetím osobám.

Kritické prostory Nemocnice Prachatice, a.s. jsou monitorovány kamerovým systémem, jehož provoz musí externí pracovníci respektovat.

4.2.Ochrana zařízení

Externí subjekty musí zacházet se zařízeními Nemocnice Prachatice, a.s. bezpečným způsobem a dodržovat následující podmínky:

a) Servery, síťové prvky a další kritická technologická zařízení se nacházejí v zabezpečených a přístupově omezených místnostech, do kterých mají externí pracovníci přístup pouze po autorizaci.
b) Externí zaměstnanci nesmí přemisťovat, odpojovat ani jinak manipulovat s technickým vybavením Nemocnice Prachatice, a.s. bez výslovného souhlasu pověřené osoby.
c) Je zakázáno připojovat neautorizované zařízení do infrastruktury Nemocnice Prachatice, a.s. (např. notebooky, USB zařízení, mobilní přístupové body).
d) V prostorách s technologickými zařízeními platí povinnost dodržovat pokyny pověřených pracovníků, bezpečnostní režim a pravidla uvedená v provozní dokumentaci.
e) Externí subjekty musí respektovat, že provoz kritických zařízení je chráněn záložními zdroji energie, a nesmí provádět činnosti, které by mohly ovlivnit jejich funkčnost.

5. Řízení změn

Externí subjekt mohou provádět změny na systémech, infrastruktuře nebo službách Nemocnice Prachatice, a.s. pouze po předchozím schválení a v souladu s procesem řízení změn.

6. Požadavky v rámci akvizice, vývoje a údržby

Externí subjekt, které zajišťují dodávku, vývoj nebo údržbu systémů, aplikací či služeb pro Nemocnice Prachatice, a.s., jsou povinny dodržovat níže uvedené bezpečnostní požadavky.

6.1. Bezpečnostní požadavky při akvizici:

Externí subjekt musí:

a) dodržovat základní bezpečnostní standardy,
b) oznamovat zjištěné zranitelnosti,
c) aplikovat bezpečnostní aktualizace
d) poskytnout dokumentaci vztahující se k předmětu smlouvy nebo dodávky.

7. Správa dokumentu

Za aktuálnost dokumentu, obsahovou správnost a pravidelnou revizi odpovídá manažer kybernetické bezpečnosti. Dokument je minimálně jednou ročně přezkoumán a v případě potřeby aktualizován, aby odrážel změny legislativy, interních procesů, technologií nebo bezpečnostních požadavků.

Dnem účinnosti nové verze dokumentu automaticky pozbývá platnosti verze předchozí.