NEMOCNICE PRACHATICE a.s.

Bezpečnostní pravidla pro významné 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
MFA	Dvoufaktorová 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 Nemocnice 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 zavést formální systém řízení bezpečnosti informací (ISMS), který jasně definuje odpovědnosti jednotlivých rolí, včetně role odpovědné za kybernetickou bezpečnost. Musí být určena osoba nebo útvar odpovědný za dohled nad plněním bezpečnostních požadavků ve vztahu k organizaci a za komunikaci v případě změn, incidentů či bezpečnostních událostí. Externí subjekt je povinen zajistit, aby všichni jeho pracovníci, kteří se podílejí na plnění smluvních závazků, byli prokazatelně proškoleni v oblasti kybernetické bezpečnosti.

Personálně obsazeny musí být ze strany následující funkce / role:

- Manažer kybernetické bezpečnosti
  - Zajišťuje komunikaci s dodavateli v oblasti bezpečnosti informací.
  - Poskytuje a schvaluje bezpečnostní požadavky, které jsou závazné pro externí subjekty.
  - Je kontaktním bodem pro řešení bezpečnostních incidentů dodavatelů.
- Architekt kybernetické bezpečnosti
  - Posuzuje technické návrhy dodavatelů z pohledu bezpečnosti.
  - Konzultuje bezpečnostní opatření, která musí dodavatel implementovat.
  - Spolupracuje s dodavateli při řízení rizik u systémů, které dodavatel ovlivňuje nebo spravuje.
- Auditor kybernetické bezpečnosti
  - Provádí audity zaměřené na dodržování bezpečnostních požadavků organizace.
  - Informuje vedení organizace o zjištěních a doporučuje nápravná opatření.
- Garant aktiv
  - Koordinuje činnosti s dodavateli, pokud se týkají správy nebo provozu konkrétních aktiv.
  - Sleduje, zda dodavatelé dodržují stanovená bezpečnostní opatření na úrovni aktiv.
  - Schvaluje přístup dodavatelů k příslušným aktivům.

2.2. Požadavky ve smluvních vztazích s externími dodavateli

Externí subjekty musí zajistit, aby jakýkoli přístup třetích stran (např. vzdálený přístup k informačnímu systému a informacím, časově omezené zásahy nebo jiné obdobné činnosti externích servisních pracovníků) byl upraven:

a) vždy smluvně,
b) v souladu s touto bezpečnostní politikou,

c) tak, aby byla zajištěna bezpečnost ICT a informací uvnitř i vně Nemocnice Prachatice, a.s.
d) Požadavky na ochranu ICT a informací podle těchto pravidel (tj. primárním nebo podpůrným aktivům) musí být zakotveny ve smluvních ujednáních s třetími stranami:
   - ještě předtím, než bude povolen a aktivován schválený přístup,
   - pouze v rozsahu nezbytném pro výkon smluvních závazků,
   - s povinnou mlčenlivostí (tzv. NDA), případně i s požadavkem adresnosti, tj. jmenovitého uvedení fyzických osob, kterým má být přidělen přístup a oprávnění.

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. Externí subjekt je povinen průběžně zajišťovat také pravidelná opakovací školení a vést o nich evidenci.

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 manažera kybernetické bezpečnosti a 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,
- poskytnout závěrečnou zprávu o zabezpečení.

Nemocnice Prachatice, a.s. může provádět kontrolu, zda byly splněny všechny bezpečnostní požadavky formou zákaznických auditů.

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) Udržovat dokumentaci, která prokazuje plnění bezpečnostních opatření.
5) Nepoužívat subdodavatele bez předchozího schválení Nemocnice Prachatice, a.s.
6) 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) audity (interní i externí),
c) 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.

Správa identit zahrnuje také řízení životního cyklu uživatelů – tj. vytváření účtů, úpravu oprávnění a okamžité zrušení přístupu při ukončení spolupráce či změně role. Veškeré změny a přidělení oprávnění musí být zaznamenávány a uchovávány pro účely auditu.

3.2.Řízení přístupu a bezpečnost práce v interní síti

3.2.1. Účel řízení přístupu

Účelem této části dokumentu je stanovit závazná pravidla pro externí subjekty při získávání, využívání a správě přístupových práv k informačním aktivům Nemocnice Prachatice, a.s., a to zejména:

a) princip minimálních oprávnění a potřeby znát (need-to-know),
b) požadavky na nastavování přístupových práv pro uživatele externích subjektů, včetně privilegovaných účtů,
c) fáze životního cyklu přístupových práv,
d) pravidla pro používání technologických účtů,
e) zásady pro udělování a omezení privilegovaných oprávnění,
f) proces řízení přístupů v mimořádných situacích,
g) způsob a četnost kontrol přístupových práv.

Externí subjekty jsou povinny tato pravidla striktně dodržovat při jakémkoli přístupu k systémům, službám nebo informacím Nemocnice Prachatice, a.s.

3.2.2. Pravidla a požadavky na řízení přístupu

1) Odpovědnosti:
    a) Garant aktiva Nemocnice Prachatice, a.s. stanovuje pravidla přístupu k jednotlivým aktivům, k nimž mohou mít uživatelé externího subjektu přístup.
    b) Provozovatel informačního systému určuje technická pravidla a kontrolní mechanismy přístupu.
    c) Externí subjekty jsou povinny přístupová práva využívat pouze v souladu s těmito pravidly a umožnit Nemocnice Prachatice, a.s. jejich průběžnou kontrolu.

2) Identifikace a evidence uživatelů externího subjektu:
    a) každý uživatel využívající přístup k systémům Nemocnice Prachatice, a.s. je jednoznačně identifikován,
    b) existuje úplná evidence všech účtů jejich zaměstnanců či subdodavatelů, kteří mají přístup,
    c) účty nejsou sdíleny a každý uživatel má vlastní autentizační údaje,
    d) používají pouze schválené účty – žádné neauditované nebo skupinové účty nejsou povoleny.

3) Záznamy a monitorování:
    a) všechny přístupy a pokusy o přístup jsou automaticky monitorovány a zaznamenávány,

b) záznamy jsou uchovávány minimálně 18 měsíců u systémů kritické infrastruktury a 12 měsíců u ostatních systémů,
c) při nečinnosti uživatele musí dojít k automatickému uzamčení obrazovky a pro odemknutí je vyžadována opětovná autentizace.

4) Přidělování a správa přístupových práv:
   a) přístupová práva jsou přidělována pouze v rozsahu nezbytném pro plnění smluvních povinností,
   b) každý přístupový požadavek musí být zdokumentovaný a schválený,
   c) přidělování přístupů probíhá podle definovaného a řízeného procesu,
   d) pro každý systém existuje definovaný přehled uživatelských rolí a oprávnění,
   e) pravidelné kontroly přístupových práv probíhají minimálně jednou ročně, případně při každé změně role uživatele dodavatele,
   f) evidence přístupů a pokusů o přístup musí být úplná a přístupná ke kontrole Nemocnice Prachatice, a.s.

3.2.3. Princip minimálních oprávnění (need-to-know)

Externí subjekty musí respektovat tyto zásady:

a) uživatel dodavatele má přístup pouze k těm aktivům, která nezbytně potřebuje k plnění své smluvní činnosti,
b) oprávnění jsou přidělena na základě definovaných rolí a jsou minimalizována,
c) veškeré změny přístupových práv musí být řízeny, zdůvodněny a schváleny.

3.2.4. Minimální požadavky na systém řízení přístupu externích subjektů

Externí subjekt musí mít zavedený interní proces řízení přístupů, který obsahuje minimálně:

a) popis uživatelských rolí a jejich oprávnění,
b) požadavky na školení osob s přístupem,
c) definici zakázaných kombinací rolí,
d) řízený proces přidělování a rušení přístupových práv,
e) technologii ověřování identity uživatelů,
f) pravidla bezpečného chování při práci s přístupovými údaji,
g) definovaný životní cyklus přístupových údajů,
h) povinné vynucování ověřování identity.

Externí subjekt musí být schopen tyto procesy prokázat na vyžádání Nemocnice Prachatice, a.s.

3.2.5. Životní cyklus řízení přístupu

1) Řízení přístupu je dokumentováno pro každé aktivum a probíhá ve fázích:
   a) žádost o přidělení přístupových práv,
   b) schvalování a přidělení přístupových práv,
   c) pravidelná kontrola přístupových práv,
   d) změna přístupových práv,

e) zrušení přístupových práv.

2) V žádosti o přidělení přístupových práv jsou definovány minimálně:
   a) osoba oprávněna žádat,
   b) uživatel,
   c) rozsah oprávnění a jejich zdůvodnění,
   d) doba platnosti oprávnění.

3) V procesu schvalování a přidělení přístupových práv je definován minimálně:
   a) osoby oprávněné schválit požadavek,
   b) schvalovací lhůty,
   c) osoby nastavující příslušná oprávnění.

4) V procesu změny přístupových práv je definována minimálně:
   a) osoba oprávněna žádat,
   b) uživatel,
   c) požadavek na změnu rozsahu oprávnění,
   d) doba platnosti oprávnění,
   e) osoby oprávněné schválit požadavek,
   f) schvalovací lhůty,
   g) osoby nastavující příslušná oprávnění.

5) Ke zrušení přístupových práv k informacím a aktivům dochází:
   a) při ukončení nebo změně pracovního nebo smluvního vztahu nebo výkonu role uživatele,
   b) na základě procesů definovaných v provozní dokumentaci jednotlivého aktiva.

3.3.Zálohování dat

Externí subjekty musí zajistit, aby:

a) byla zálohována všechna důležitá data nezbytná pro zajištění kontinuity provozu jimi spravovaných systémů nebo v rámci jimi poskytovaných ICT služeb, a to vhodnou definicí požadavků na zálohy,
b) se na lokálních počítačových stanicích nevyskytovaly žádné informace určené ke sdílení a podléhající centrálnímu zálohování.

Vyžaduje-li to charakter zpracování, jsou individuální zálohy dat na lokálních PC (např. u specifických lokálních agend) řešeny jednotlivě dle požadavků garantů těchto aktiv.

Pokud na straně externích subjektů existují záložní kopie důležitých informací, musí být zabezpečeny před neoprávněným přístupem.

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.

1) Nemocnice Prachatice, a.s. má formálně definovaný proces řízení změn, který se vztahuje na:
   a) informační systémy,
   b) síťovou infrastrukturu,

c) aplikace a služby provozované nebo spravované externím subjektem.

2) Externí subjekty jsou povinny mají povinnost dodržovat zavedený proces řízení změn:
   a) provádět jakékoli změny pouze na základě předchozího schválení,
   b) postupovat dle procesů Nemocnice Prachatice, a.s. pro plánování, schvalování, implementaci, dokumentaci a archivaci změn,
   c) spolupracovat při poskytování potřebných informací o plánovaných změnách.

3) Hodnocení dopadu a rizik před provedením jakékoliv změny jsou externí subjekty povinny:
   a) poskytnout Nemocnice Prachatice, a.s. informace potřebné k vyhodnocení dopadu změny na bezpečnost a kontinuitu provozu,
   b) umožnit provedení analýzy rizik, případně dodat vlastní analýzu, pokud to Nemocnice Prachatice, a.s. vyžaduje,
   c) přijmout a implementovat opatření pro mitigaci identifikovaných rizik.

4) Schvalování a dokumentace:
   a) Změny lze realizovat pouze dle schváleného plánu a před nasazením do produkčního prostředí musí být řádně otestovány z hlediska funkčnosti i bezpečnosti.
   b) Každá provedená změna musí být dokumentována, včetně popisu, data provedení, schválení a výsledků testů. Dokumentace slouží jako podklad pro auditní účely.
   c) Nemocnice Prachatice, a.s. provádí pravidelné kontroly a audity procesu řízení změn. Externí subjekty jsou povinny poskytovat součinnost a přijmout případná nápravná opatření vyplývající z výsledků těchto kontrol.

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 splnit bezpečnostní požadavky definované Nemocnice Prachatice, a.s. již ve fázi výběru. Smluvní dokumentace musí obsahovat zejména:

a) povinnost dodržovat stanovené bezpečnostní standardy (např. ISO/IEC 27001, OWASP),
b) povinnost provádět bezpečnostní testy před uvedením dodaných systémů do provozu,
c) povinnost neprodleně hlásit identifikované zranitelnosti a bezpečnostní incidenty.

6.2. Bezpečnost ve fázi vývoje

Externí subjekty musí uplatňovat princip Security by Design a zajistit:

a) zahrnutí bezpečnostních požadavků do návrhu systémů a aplikací,
b) používání bezpečnostních standardů pro vývoj (např. OWASP Top 10).

c) Veškerý nový nebo upravený software dodaný externím subjektem musí projít:
   - statickou a dynamickou analýzou kódu,
   - penetračními testy před nasazením do provozu.

d) Externí subjekt musí poskytnout výsledky testů a nápravná opatření.

6.3. Údržba a aktualizace

1) Externí subjekty zajišťující údržbu musí:
   a) aplikovat bezpečnostní záplaty a aktualizace v termínech stanovených Nemocnice Prachatice, a.s.,
   b) testovat aktualizace před nasazením,
   c) dokumentovat veškeré údržbové zásahy v souladu s požadavky Nemocnice Prachatice, a.s.

2) Externí subjekty jsou povinny spolupracovat na bezpečnostním hodnocení provozovaných řešení, které zahrnuje zejména:
   a) pravidelné penetrační testy,
   b) pravidelné nebo ad-hoc skeny zranitelností.

3) Externí subjekty musí vést a na vyžádání předat dokumentaci zahrnující:
   a) splněné bezpečnostní požadavky,
   b) testovací a validační protokoly,
   c) záznamy o změnách, verzích a aktualizacích,

Dokumentace musí být archivována, úplná a dostupná pro auditní účely organizace.

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.