Nemocnice Nové Město na Moravě, příspěvková organizace

Žďárská 610

592 31 Nové Město na Moravě

Bezpečnostní a technické standardy ICT NNM

Datum vydání:	**10.9.2026**
Verze:	**01**
Počet stran:	**19**

Autor:	**Jan Sobotka**
	Manažer kybernetické bezpečnosti
Schválila:	**JUDr. Věra Palečková**
	Ředitelka nemocnice Nové Město na Moravě, p.o.

Požadavky tohoto dokumentu vycházejí z bezpečnostních opatření ISMS nemocnice, řízení rizik a požadavků právních předpisů v oblasti kybernetické bezpečnosti.

1. Účel dokumentu

Tento dokument stanovuje minimální technické, bezpečnostní a provozní standardy pro návrh, implementaci, provoz, podporu a správu ICT systémů a technologií v prostředí Nemocnice Nové Město na Moravě (NNM).

Tento dokument se vztahuje také na technologie a systémy, které nejsou primárně označeny jako ICT, pokud využívají síťovou komunikaci, zpracovávají data nebo se napojují na infrastrukturu objednatele. O zařazení konkrétního řešení do působnosti tohoto dokumentu rozhoduje příslušný ICT útvar objednatele.

Dokument je závazný zejména pro dodavatele ICT řešení, pro interní útvary nemocnice podílející se na pořizování, zadávání, implementaci, provozu, správě nebo kontrole ICT systémů a pro další subjekty, které se podílejí na provozu, správě nebo integraci ICT systémů. Za odborné posouzení technického souladu a kontrolu dodržování požadavků odpovídá úsek informatiky ve spolupráci s manažerem kybernetické bezpečnosti, pokud není stanoveno jinak.

Dokument je využíván zejména:

- jako součást zadávací nebo smluvní dokumentace veřejných zakázek v rozsahu nezbytném pro dané plnění,
- jako minimální bezpečnostní a technický standard ICT prostředí nemocnice,
- jako návazná bezpečnostní dokumentace ke směrnici č. 2/2022 Systém řízení bezpečnosti informací a k ISMS nemocnice.

Pokud jsou dodavatelům, uchazečům nebo jiným třetím stranám poskytovány části dokumentace obsahující citlivé bezpečnostní nebo provozní informace, poskytují se pouze způsobem stanoveným objednatelem a při zajištění odpovídající mlčenlivosti nebo ochrany informací.

V případě, že je pro konkrétní veřejnou zakázku zpracována samostatná technická specifikace, jsou požadavky tohoto dokumentu považovány za minimální závazný standard, který je touto samostatnou technickou specifikací dále rozpracován, zpřesněn nebo rozšířen. Příslušný ICT útvar objednatele odpovídá za odborné posouzení souladu technické specifikace, zadávací dokumentace a smluvních podmínek s tímto dokumentem. V případě rozporu mezi obecnými požadavky tohoto dokumentu a konkrétní technickou specifikací se použije přísnější požadavek, pokud objednatel nestanoví jinak.

Tento dokument nestanovuje konkrétní technickou implementaci řešení v prostředí objednatele na úrovni detailní konfigurace nebo interní architektury; tyto informace mohou být součástí technické specifikace konkrétní veřejné zakázky nebo jiné neveřejné dokumentace objednatele.

Tyto bezpečnostní a technické požadavky tvoří součást zadávací nebo smluvní dokumentace v rozsahu, v jakém jsou do konkrétní veřejné zakázky nebo smlouvy zahrnuty. Dodavatel je povinen je zohlednit již při přípravě nabídky a při realizaci plnění. Splnění relevantních požadavků posuzuje příslušný ICT útvar objednatele při přípravě zadávací dokumentace, při posouzení nabídek, při implementaci a před převzetím plnění. Nesplnění požadavků může být důvodem k vyloučení nabídky, odmítnutí převzetí plnění nebo uplatnění smluvních sankcí, pokud to vyplývá ze zadávací nebo smluvní dokumentace a právních předpisů.

Dodavatel je povinen tyto požadavky zohlednit již při přípravě nabídky; případná technická omezení nebo nemožnost splnění požadavku musí být výslovně uvedena v nabídce nebo v žádosti o vysvětlení zadávací dokumentace.

Pro lepší orientaci dodavatelů jsou konkrétní technické a provozní požadavky dále rozvedeny v jednotlivých kapitolách tohoto dokumentu.

Dokument je určen k poskytování jako celek, pokud objednatel neurčí z důvodů ochrany bezpečnostních informací jinak. Případné výňatky nebo zkrácené znění připravuje nebo schvaluje příslušný ICT útvar objednatele tak, aby nedošlo ke zkreslení významu požadavků.

Dokument je nutné posuzovat jako celek.

2. Rozsah a působnost

Tento dokument se vztahuje na všechny dodavatele poskytující software (on-premise i cloud), hardware, integrační, analytické, servisní a vývojové služby, jakož i služby podpory, údržby a provozu ICT systémů. Dokument stanovuje obecné technické a bezpečnostní požadavky uvedené zejména v kapitolách 1 až 21 a může být použit jako samostatná technická specifikace nebo jako její základ. Specifické požadavky pro jednotlivé typy systémů jsou uvedeny v kapitole 22 tohoto dokumentu; tyto požadavky doplňují obecné požadavky tohoto dokumentu. V případě rozporu mezi obecnými požadavky a specifickými požadavky podle typu systému se použije přísnější požadavek, pokud objednatel nestanoví jinak.

Veškeré návrhy řešení, které zahrnují napojení na ICT infrastrukturu objednatele, podléhají předchozímu schválení příslušného ICT útvaru objednatele (úsek informatiky, manažer kybernetické bezpečnosti). O zařazení řešení do působnosti tohoto dokumentu, o jeho napojení na ICT infrastrukturu objednatele a o aplikaci jednotlivých požadavků rozhoduje výhradně tento útvar, který současně rozhoduje o jejich interpretaci a rozsahu aplikace; toto rozhodnutí je závazné pro všechny organizační útvary objednatele i dodavatele.

Požadavky tohoto dokumentu jsou aplikovány přiměřeně s ohledem na charakter systému, jeho význam, klasifikaci a výsledky řízení rizik, přičemž rozsah a přísnost jednotlivých požadavků se může lišit podle typu řešení. V rámci zadávacího řízení je dodavatel povinen vycházet z tohoto dokumentu jako ze závazné části zadávací dokumentace; pokud je součástí veřejné zakázky samostatná technická specifikace, je dodavatel povinen splnit jak požadavky této specifikace, tak požadavky tohoto dokumentu.

Dodavatel je povinen při zpracování nabídky zohlednit všechny požadavky tohoto dokumentu a v případě nejasností požádat o vysvětlení zadávací dokumentace. Za správnost a jednoznačnost zadávací dokumentace odpovídá zadavatel; případné rozpory nebo nejasnosti zadávací dokumentace se řeší postupem stanoveným právními předpisy a pravidly zadávacího řízení. Konečné posouzení splnění požadavků tohoto dokumentu a jejich aplikace na konkrétní řešení provádí ICT útvar objednatele; toto posouzení je podkladem pro rozhodnutí zadavatele.

3. Legislativní rámec

Dodavatel je povinen navrhnout a dodat řešení v souladu s platnými právními předpisy tak, aby umožňovalo objednateli plnit povinnosti vyplývající ze zákona č. 264/2025 Sb., včetně řízení kybernetických rizik (§ 13), zavádění bezpečnostních opatření (§ 15) a hlášení kybernetických bezpečnostních incidentů (§ 18 a násl.), dále z vyhlášek č. 408-411/2025 Sb., zákona č. 372/2011 Sb., nařízení GDPR (zejména čl. 6, 9, 28, 32 a 35), zákona č. 110/2019 Sb., zákona č. 106/1999 Sb. v rozsahu poskytování informací a interních bezpečnostních předpisů NNM.

Dodavatel je povinen zajistit, aby dodané řešení tyto povinnosti nejen formálně umožňovalo, ale také je prakticky podporovalo v rozsahu odpovídajícím jeho účelu a charakteru.

4. Klasifikace systému a dat

Dodavatel je povinen poskytnout součinnost objednateli při klasifikaci dodávaného systému a zpracovávaných dat z hlediska jejich významu pro důvěrnost, integritu a dostupnost. Na vyžádání objednatele je dodavatel povinen poskytnout zejména popis funkcí systému a jeho účelu, popis zpracovávaných dat včetně určení, zda se jedná o osobní údaje, zvláštní

kategorie osobních údajů nebo jiné citlivé informace, popis závislostí systému na dalších systémech a infrastruktuře a popis dopadů nedostupnosti, narušení integrity nebo úniku dat.

Na základě těchto informací provádí objednatel klasifikaci systému a stanovuje bezpečnostní požadavky v souladu s řízením rizik podle § 13 zákona č. 264/2025 Sb. Dodavatel je povinen tuto klasifikaci a z ní vyplývající bezpečnostní požadavky respektovat.

5. Řízení privilegovaných přístupů

Detailní požadavky na autentizaci, správu hesel a identit jsou dále uvedeny v kapitole 24.2.

Dodavatel je povinen zajistit, aby veškeré privilegované přístupy k systému (zejména administrátorské, servisní nebo integrační účty) byly jednoznačně evidovány, přiřazeny ke konkrétní fyzické osobě, řízeny a auditovány, přičemž privilegované účty nesmí být sdílené mezi více osobami, pokud to není technicky nezbytné; v takovém případě musí být zajištěna jednoznačná dohledatelnost konkrétní osoby, která přístup využila.

Používání privilegovaných účtů musí být omezeno na nezbytný rozsah a dobu a musí být využíváno výhradně pro účely správy a údržby systému, přičemž přístupy musí být technicky zabezpečeny, zejména použitím vícefaktorového ověření, pokud to povaha systému umožňuje.

Dodavatel je povinen zajistit evidenci a auditní stopu všech operací provedených s využitím privilegovaných přístupů a na vyžádání objednatele umožnit kontrolu jejich využívání, včetně předložení relevantních logů; vzdálený přístup s privilegovanými oprávněními musí být vždy předem schválen objednatelem, časově omezen, realizován zabezpečeným způsobem a plně auditovatelný.

Objednatel si vyhrazuje právo omezit nebo odebrat privilegované přístupy dodavatele, pokud to vyžaduje bezpečnostní situace.

6. Kategorizace dodávaného řešení z pohledu NIS2

6.1 Zařazení do režimu

Nemocnice Nové Město na Moravě je poskytovatelem regulované služby ve zdravotnictví a spadá do režimu vyšších povinností dle vyhlášky č. 408/2025 Sb. Systémy, které mají dopad na poskytování zdravotních služeb nebo jsou na ně provozně či datově navázány, se zpravidla považují za součást regulované služby v režimu vyšších povinností, pokud není na základě řízení rizik stanoveno jinak.

6.2 Omezená možnost nižšího režimu

Zařazení systému do nižšího režimu je možné pouze ve výjimečných případech na základě řízení rizik, zejména pokud systém nepředstavuje regulovanou službu, není významně provozně ani datově navázán na poskytování zdravotní péče, nepracuje s osobními údaji pacientů a jeho výpadek nemá dopad na dostupnost zdravotních služeb. O zařazení rozhoduje objednatel.

6.3 Dopad na povinnosti dodavatele

Standardním režimem je režim vyšších povinností, který vyžaduje splnění požadavků dle vyhlášky č. 409/2025 Sb. Výjimečně může být systém zařazen do režimu nižších povinností. Dodavatel je povinen poskytnout objednateli pravdivé, úplné a aktuální informace nezbytné pro zařazení systému do příslušného režimu, zejména informace o architektuře, zpracovávaných datech, závislostech a dopadech na dostupnost služeb.

7. Bezpečnost dodavatelského řetězce

Dodavatel je povinen zajistit, že bezpečnostní požadavky tohoto dokumentu budou uplatněny i vůči jeho subdodavatelům, pokud se podílejí na plnění předmětu veřejné zakázky, a odpovídá za jejich plnění, jako by je plnil sám. Zapojení subdodavatelů nebo změna dodavatelského řetězce, která může mít dopad na bezpečnost nebo provoz systému, podléhá předchozímu schválení objednatelem.

Dodavatel je povinen na vyžádání objednatele poskytnout informace o zapojení subdodavatelů, zejména pokud mají přístup k systému, datům nebo infrastruktuře objednatele, a doložit, jakým způsobem řídí jejich bezpečnost.

Pokud je součástí řešení využití cloudových služeb, externích platforem nebo jiných služeb třetích stran, je dodavatel povinen tuto skutečnost výslovně uvést, včetně identifikace poskytovatele služby, umístění zpracování dat a popisu způsobu zabezpečení. Dodavatel je povinen zajistit, aby externí služby neohrozily dostupnost, integritu nebo důvěrnost systému a aby byla identifikována a řízena rizika spojená s jejich využíváním.

8. Požadavky na identitu a řízení přístupů (AD / IDM)

8.1 Autentizace

Dodavatel je povinen podporovat standardní mechanismy autentizace používané v prostředí objednatele, zejména LDAP/LDAPS, Kerberos, SAML 2.0 (SSO), OpenID Connect (OIDC) nebo jiné kompatibilní mechanismy (např. RADIUS), aby byla zajištěna jednotná autentizace v rámci infrastruktury NNM. Přístupy musí být technicky zabezpečeny, zejména použitím vícefaktorového ověření, pokud to povaha systému umožňuje nebo pokud objednatel nestanoví jinak. Konkrétní způsob integrace do identitní infrastruktury objednatele stanoví objednatel s ohledem na charakter systému a výsledek řízení rizik.

8.2 Autorizace a řízení přístupů na základě rolí

Dodavatel je povinen podporovat řízení přístupů na základě rolí (RBAC), umožnit mapování těchto rolí na skupiny v Active Directory a zajistit dostatečnou granularitu oprávnění odpovídající principu nejmenších oprávnění. Systém nesmí obsahovat žádné hard-coded účty ani pevně uložené přístupové údaje.

8.3 Administrátorské účty

Administrátorské činnosti musí být, pokud to povaha systému umožňuje nebo pokud objednatel nestanoví jinak, prováděny prostřednictvím účtů spravovaných v Active Directory. Lokální účty mohou být použity pouze v případě nouzového přístupu, a to za podmínky použití vícefaktorového ověření a bezpečného uložení přístupových údajů v trezoru hesel.

8.4 Výjimka pro AD

Požadavky na využití Active Directory se nepoužijí na systémy, u nichž by jejich aplikace byla v rozporu s bezpečnostním nebo provozním charakterem systému (zejména OT nebo autonomní systémy), pokud objednatel nestanoví jinak.

Bezpečnostní požadavky na autentizaci, hesla a vícefaktorové ověření jsou dále specifikovány v kapitole 24.2.

9. Logování a monitoring (SIEM)

Dodávané řešení musí poskytovat logy ve standardizovaných formátech, jako je syslog, JSON nebo CEF, zaznamenávat klíčové bezpečnostní události včetně autentizace, autorizace, změn konfigurace, administrátorských zásahů, chybových stavů a volání API a podporovat odesílání logů do log-forwarderu nebo do systému Elastic SIEM v prostředí NNM, pokud to povaha systému umožňuje. Logy musí obsahovat dostatečné informace pro identifikaci události, zejména identitu uživatele nebo systému, čas události a popis provedené akce. Součástí požadavků je zajištění správné časové synchronizace

prostřednictvím NTP serverů NNM. Pokud systém technicky neumožňuje splnění těchto požadavků, je dodavatel povinen tuto skutečnost doložit a navrhnout odpovídající kompenzační opatření, která podléhají schválení objednatelem.

Pokud systém technicky neumožňuje přímé předávání logů do SIEM objednatele, je dodavatel povinen tuto skutečnost uvést a navrhnout alternativní způsob zajištění auditovatelnosti a dostupnosti logů, přičemž musí být zajištěn přímý, nepřetržitý a auditovatelný přístup objednatele k těmto logům bez závislosti na součinnosti dodavatele.

Logy musí být dostupné bez zbytečného prodlení a uchovávány po dobu stanovenou objednatelem nebo právními předpisy, minimálně však po dobu 6 měsíců, pokud není stanoveno jinak, a musí být chráněny proti neoprávněné manipulaci, smazání nebo ztrátě.

10. Zajištění dostupnosti a obnovy provozu

Dodavatel je povinen navrhnout a dodat systém tak, aby byla zajištěna jeho dostupnost v rozsahu odpovídajícím jeho účelu a významu pro provoz objednatele. Dodavatel je povinen definovat základní parametry obnovy systému, zejména maximální přípustnou dobu obnovy provozu (RTO – Recovery Time Objective) a maximální přípustnou ztrátu dat (RPO – Recovery Point Objective), které musí odpovídat charakteru systému a požadavkům objednatele.

Dodavatel je povinen popsat a implementovat postupy obnovy systému po havárii, kybernetickém incidentu nebo jiné mimořádné události, včetně závislostí na infrastruktuře, třetích stranách nebo externích službách. Pokud systém ukládá data, musí být zajištěno jejich pravidelné zálohování v rozsahu odpovídajícím jejich významu; zálohy musí být chráněny proti neoprávněnému přístupu, ztrátě a kompromitaci a musí být testována jejich obnovitelnost.

Dodavatel je povinen uvést, zda systém umožňuje provoz v omezeném režimu při výpadku některých komponent nebo konektivity, a popsat omezení tohoto režimu. Dodavatel je povinen doložit, že postupy obnovy byly testovány, nebo poskytnout součinnost při jejich ověření objednatelem.

Rozsah požadavků na dostupnost a obnovu se stanoví s ohledem na klasifikaci systému a výsledek řízení rizik podle § 13 zákona č. 264/2025 Sb. U systémů s dopadem na poskytování zdravotních služeb musí být dostupnost a obnova navržena tak, aby nedošlo k ohrožení poskytování zdravotní péče. Dodavatel je povinen uvést závislosti systému na externích službách nebo konektivitě.

Rozsah požadavků musí být zohledněn již v návrhu řešení a uveden v nabídce dodavatele.

11. Řízení zranitelností a bezpečnostních slabin

Dodavatel je povinen průběžně sledovat zranitelnosti a bezpečnostní slabiny dodaného řešení a bez zbytečného odkladu, nejpozději však do 24 hodin po jejich zjištění, informovat objednatele o zranitelnostech, které mohou mít dopad na bezpečnost, dostupnost nebo integritu systému. Tato povinnost oznámení zranitelností není dotčena povinností hlášení bezpečnostních incidentů dle kapitoly 17 ani plněním SLA dle kapitoly 13. Dodavatel je povinen zajistit jejich odstranění nebo mitigaci a současně poskytnout objednateli součinnost při jejich řešení, včetně návrhu nápravných opatření a časového harmonogramu.

Dodavatel je povinen poskytovat bezpečnostní aktualizace a opravy (patches) po dobu životního cyklu dodaného řešení a zajistit, aby jejich aplikace neohrozila provoz systému, pokud objednatel nestanoví jinak. V případě, že zranitelnost vedla nebo mohla vést k bezpečnostnímu incidentu, postupuje se zároveň podle kapitoly 17 tohoto dokumentu. Tyto požadavky se uplatňují souběžně s požadavky na řešení incidentů dle kapitoly 17 a SLA dle kapitoly 13.

Zranitelnost, bezpečnostní incident a provozní incident jsou posuzovány nezávisle a mohou nastat souběžně.

12. Požadavky na implementaci

12.1 Dokumentace

Dodavatel je povinen tyto informace poskytnout již v rámci nabídky v rozsahu odpovídajícím fázi návrhu řešení.

Dodavatel je povinen poskytnout kompletní instalační a provozní dokumentaci, bezpečnostní doporučení, přehled datových toků a seznam všech potřebných oprávnění v Active Directory, databázích a síťové infrastruktuře.

12.2 Konfigurace

Dodavatel je povinen předat úplnou a aktuální konfiguraci systému, přehled provedených změn v infrastruktuře, seznam vytvořených technických a uživatelských účtů a seznam všech API a integračních rozhraní, která systém využívá.

12.3 Připojování zařízení do sítě objednatele

Každé zařízení připojované do síťové infrastruktury objednatele musí být předem schváleno objednatelem. Není přípustné připojení neautorizovaných, neznámých nebo předem neschválených zařízení do sítě objednatele. Dodavatel je povinen před zahájením realizace poskytnout seznam všech zařízení, která budou připojena do infrastruktury objednatele, včetně údajů nezbytných pro jejich jednoznačnou identifikaci a schválení. Minimální rozsah identifikace zařízení zahrnuje typ zařízení, jeho účel, umístění a jednoznačný identifikátor zařízení. MAC adresa může být využita jako identifikátor zařízení, zejména u systémů, které neumožňují silnější formu autentizace; v takovém případě musí být její použití omezeno a doplněno dalšími bezpečnostními opatřeními na úrovni infrastruktury (např. segmentace, řízení komunikace, monitoring). MAC adresa nesmí být považována za plnohodnotný bezpečnostní autentizační mechanismus. U zařízení, která podporují pokročilejší autentizaci (např. 802.1X), musí být MAC adresa využívána pouze jako dočasný nebo doplňkový mechanismus (např. při prvotním připojení), přičemž následná autentizace musí být realizována silnější metodou (např. certifikátem). Bez poskytnutí těchto údajů nebude zařízení připojeno do infrastruktury objednatele.

Přístup zařízení do sítě musí být řízen prostřednictvím mechanismů autentizace a autorizace zařízení a uživatelů. Zařízení musí být jednoznačně identifikovatelná a jejich přístup musí být omezen pouze na nezbytný rozsah odpovídající jejich funkci. Zařízení jsou po připojení zařazována do odpovídajících síťových segmentů podle rozhodnutí objednatele. Komunikace zařízení musí být řízena a omezena prostřednictvím bezpečnostních mechanismů sítě, zejména s ohledem na princip minimálních oprávnění a omezení komunikace pouze na nezbytné služby a systémy. Systém ani jeho komponenty nesmí vyžadovat obcházení bezpečnostních opatření objednatele, přímý nebo neřízený přístup do sítě, ani otevření neomezené komunikace do vnějších sítí (např. internetu). Veškerá komunikace musí být realizována v souladu s bezpečnostní politikou objednatele a podléhá jeho schválení. Za přiřazený síťový segment se pro účely tohoto dokumentu považuje logicky oddělená část síťové infrastruktury určená objednatelem pro konkrétní typ systému nebo zařízení, ve které je komunikace řízena a omezena podle bezpečnostních požadavků objednatele. Objednatel využívá mechanismy řízení přístupu do sítě (např. 802.1X nebo NAC), a zařízení musí být schopno těmto mechanismům vyhovět, pokud objednatel nestanoví jinak. Není přípustné připojovat do infrastruktury objednatele vlastní síťové prvky dodavatele (např. routery, switche, bezdrátové přístupové body, LTE/5G zařízení), ani vytvářet paralelní nebo obcházející síťovou infrastrukturu bez výslovného schválení objednatele.

Systém nesmí obsahovat pevně definované (hard-coded) síťové adresy, přístupové body nebo komunikační parametry, které nelze měnit bez zásahu dodavatele, pokud objednatel nestanoví jinak.

Tato opatření jsou v prostředí objednatele realizována prostřednictvím nástrojů pro řízení přístupu do sítě (např. NAC).

12.4 Testování

Před převzetím řešení musí být ověřena zejména funkční integrace do identitní infrastruktury (např. Active Directory), správné zaznamenávání a dostupnost logů včetně jejich předávání do SIEM, funkčnost řízení přístupů a oprávnění, provedení bezpečnostních testů odpovídajících charakteru systému, funkčnost zálohování a obnovy (backup/restore) a v případě kritických systémů také zátěžové testy, pokud to povaha systému umožňuje, nebo pokud

objednatel nestanoví jinak. Součástí ověření je také kontrola předané dokumentace, konfigurace systému a identifikace všech integračních rozhraní a datových toků.

Testování musí být provedeno v prostředí odpovídajícím reálnému provozu nebo v prostředí objednatele, pokud objednatel nestanoví jinak.

Rozsah testování může být dále upřesněn v rámci konkrétní veřejné zakázky podle charakteru systému a výsledků řízení rizik. Požadavky na integraci do identitní infrastruktury a SIEM se nepoužijí na systémy, u nichž by jejich aplikace byla v rozporu s bezpečnostním nebo provozním charakterem systému, pokud objednatel nestanoví jinak.

Testování musí být doloženo protokolem nebo jiným průkazným a auditovatelným způsobem. Výsledky testování podléhají schválení objednatelem.

Splnění požadavků kapitoly 12 je podmínkou převzetí řešení a jejich nesplnění je důvodem k odmítnutí převzetí ze strany objednatele.

13. Požadavky na provoz, podporu a SLA

Dodavatel je povinen zajistit provozní podporu dodaného řešení v rozsahu odpovídajícím jeho významu pro provoz objednatele, zejména u systémů připojených do ICT infrastruktury objednatele nebo systémů majících dopad na poskytování zdravotních služeb. Pokud není ve smluvní dokumentaci konkrétní veřejné zakázky stanoveno jinak, platí jako minimální závazná úroveň SLA reakce na kritický incident nejpozději do 2 hodin od jeho nahlášení, zahájení řešení kritického incidentu nejpozději do 4 hodin, odstranění kritické bezpečnostní zranitelnosti nejpozději do 7 dnů a odstranění ostatních zranitelností nejpozději do 30 dnů. Klasifikaci incidentů a jejich závažnosti stanovuje objednatel.

Tyto požadavky představují minimální standard, který musí být dodavatelem splněn, přičemž konkrétní SLA a provozní podmínky mohou být dále rozpracovány ve smluvní dokumentaci, aniž by došlo ke snížení této úrovně, pokud objednatel výslovně nerozhodne jinak na základě posouzení rizik. U systémů zařazených do režimu vyšších povinností musí SLA odpovídat jejich kritičnosti a významu pro poskytování zdravotních služeb, včetně zajištění odpovídající dostupnosti podpory. U systémů s dopadem na poskytování zdravotních služeb musí být zajištěna dostupnost podpory v režimu odpovídajícím jejich kritičnosti, zpravidla v režimu 24/7, pokud objednatel nestanoví jinak.

Dodavatel je povinen v nabídce uvést způsob zajištění podpory, řešení incidentů a odstraňování zranitelností, včetně reakčních dob, dostupnosti podpory a eskalačních mechanismů, a zajistit jejich reálnou dostupnost po dobu provozu systému. Požadavky na SLA se vztahují zejména na řešení bezpečnostních incidentů dle kapitoly 17 a odstraňování zranitelností dle kapitoly 11 tohoto dokumentu. Není přípustné provozovat systém připojený do ICT infrastruktury objednatele bez definovaného a funkčního režimu podpory a řešení incidentů. Požadavky SLA se uplatní paralelně s povinností hlášení dle kapitoly 11 a 17; splnění jedné povinnosti nenahrazuje druhou.

14. Práce s daty a ochranou osobních údajů (GDPR)

Dodavatel je povinen zajistit technická a organizační opatření odpovídající požadavkům čl. 32 GDPR, zejména s ohledem na zabezpečení zpracovávaných dat, řízení přístupů a ochranu proti neoprávněnému přístupu, ztrátě nebo zneužití dat, a plnit povinnosti zpracovatele podle čl. 28 GDPR.

Dodavatel je povinen zajistit, že nedojde k přenosu osobních údajů mimo EU ani k přístupu k těmto údajům ze třetích zemí bez předchozího schválení objednatelem.

Dodavatel je povinen zajistit logování a auditovatelnost všech operací spojených s exportem nebo předáním dat a na vyžádání umožnit kontrolu těchto operací.

Dodavatel je povinen poskytnout objednateli součinnost při provádění posouzení vlivu na ochranu osobních údajů (DPIA), pokud objednatel stanoví, že je takové posouzení vyžadováno.

Dodavatel je povinen na vyžádání doložit implementovaná technická a organizační opatření.

15. Cloud a bezpečnostní úrovně dle vyhl. č. 411/2025 Sb.

Pokud řešení využívá cloudové služby, je dodavatel povinen zajistit, aby dodané řešení umožňovalo jeho zařazení do příslušné bezpečnostní úrovně (nízká, střední, vysoká nebo kritická) v souladu s vyhláškou č. 411/2025 Sb. Dodavatel je povinen poskytnout veškeré informace nezbytné pro toto zařazení, zejména informace o architektuře řešení, umístění zpracování a ukládání dat, zapojených poskytovatelích služeb a subdodavatelích.

Cloudové služby nesmí být využívány bez předchozího schválení objednatelem. Dodavatel je povinen zajistit, že využití cloudových služeb neohrozí bezpečnost, dostupnost ani integritu systému a umožní řízení rizik v rozsahu požadovaném právními předpisy a interními předpisy objednatele.

Zpracování a ukládání dat musí probíhat na území EU, pokud objednatel nestanoví jinak na základě posouzení rizik. V případě využití služeb mimo EU nebo přístupu k datům ze třetích zemí je dodavatel povinen tuto skutečnost předem oznámit, doložit právní a bezpečnostní zajištění takového přenosu a získat předchozí souhlas objednatele.

Dodavatel je povinen na vyžádání doložit, jakým způsobem jsou cloudové služby zabezpečeny, zejména prostřednictvím relevantních certifikací, auditních zpráv nebo jiných průkazných dokumentů.

16. Audity, kontrola a součinnost

Dodavatel je povinen umožnit provedení auditu ze strany objednatele nebo auditora pověřeného objednatelem, a to v rozsahu nezbytném pro ověření plnění požadavků tohoto dokumentu, včetně přístupu k relevantním informacím, dokumentaci, systémům a logům. Tato povinnost se vztahuje i na subdodavatele, pokud se podílejí na plnění předmětu veřejné zakázky.

Dodavatel je povinen poskytnout veškerou potřebnou součinnost při auditech bezpečnosti podle vyhlášek č. 409/2025 Sb. a č. 410/2025 Sb. a zajistit včasné plnění uložených nápravných opatření ve lhůtách stanovených objednatelem nebo vyplývajících z právních předpisů.

17. Řízení bezpečnostních incidentů

Povinnosti dle této kapitoly se vztahují i na incidenty vzniklé u subdodavatelů nebo v souvisejících externích službách, pokud mají dopad na dodané řešení. Dodavatel je povinen bez zbytečného odkladu, nejpozději však do 24 hodin od zjištění, informovat objednatele o jakémkoliv bezpečnostním incidentu souvisejícím s dodaným řešením, který může mít dopad na dostupnost, integritu nebo důvěrnost dat nebo na poskytování zdravotních služeb.

Dodavatel je povinen zajistit součinnost při řešení bezpečnostního incidentu, zejména poskytnout relevantní technické informace, logy, konfigurace a další podklady nezbytné pro analýzu, řešení a dokumentaci incidentu, a průběžně informovat objednatele o stavu jeho řešení.

Dodavatel je povinen zajistit, aby systém umožňoval zaznamenávání a uchování logů v rozsahu nezbytném pro detekci a vyšetřování bezpečnostních incidentů. V případě incidentu je dodavatel povinen spolupracovat s objednatelem při plnění oznamovacích povinností podle zákona č. 264/2025 Sb., zejména poskytnout součinnost při přípravě podkladů pro hlášení incidentu příslušnému orgánu.

Dodavatel je povinen přijmout bez zbytečného odkladu opatření k nápravě a minimalizaci dopadů incidentu a navrhnout opatření k zamezení jeho opakování. Dodavatel odpovídá za plnění těchto povinností svými subdodavateli, jako by je plnil sám.

Posouzení, zda se jedná o bezpečnostní incident, provádí objednatel.

Povinnosti dle této kapitoly se uplatňují nezávisle na SLA dle kapitoly 13.

18. Ukončení smlouvy a předání

Při ukončení plnění je dodavatel povinen předat kompletní a aktuální konfiguraci systému, veškerá data objednatele ve strukturované a využitelné podobě, odstranit veškerá pracovní a dočasná data, vrátit všechny poskytnuté prostředky a přístupy a ukončit veškeré přístupy do infrastruktury objednatele.

Dodavatel je povinen zajistit součinnost při předání nebo migraci systému na jiného dodavatele nebo do jiného prostředí, pokud to objednatel požaduje.

Dodavatel je povinen doložit odstranění dat objednatele ze svých systémů a systémů subdodavatelů a zajistit provedení závěrečného technického auditu tak, aby bylo možné ověřit řádné a bezpečné ukončení provozu systému.

19. Výjimky

Jakákoli výjimka z tohoto dokumentu musí být předem písemně schválena objednatelem, a to na základě posouzení příslušného ICT útvaru objednatele (úsek informatiky, manažer kybernetické bezpečnosti). Výjimky lze udělit pouze ve zdůvodněných případech na základě posouzení rizik a po potvrzení, že neohrozí bezpečnost, provoz ani soulad s legislativními požadavky.

Posouzení výjimek se provádí na základě zdůvodnění dodavatele, charakteru systému a výsledků řízení rizik. Výjimky mohou být uděleny zejména v případech, kdy požadavek není prokazatelně technicky realizovatelný nebo by jeho aplikace vedla k nepřiměřenému omezení funkčnosti systému.

Výjimky musí být evidovány a jsou udělovány na omezenou dobu nebo do splnění stanovených podmínek, pokud objednatel nestanoví jinak.

20. Klasifikace požadavků

Tento dokument využívá klasifikaci požadavků pouze v podobě označení povinných požadavků. Povinné požadavky představují závazné minimální bezpečnostní standardy, které musí být dodavatelem splněny, pokud není udělena výjimka v souladu s kapitolou 19 tohoto dokumentu.

Požadavky tohoto dokumentu se aplikují přiměřeně s ohledem na charakter systému, jeho význam a výsledky řízení rizik.

Ostatní typy klasifikace (doporučené, dobrovolné) nejsou v tomto dokumentu používány.

21. Poskytování informací dle zákona č. 106/1999 Sb.

Tento dokument obsahuje obecné technické a bezpečnostní požadavky a neobsahuje konkrétní informace o implementaci, jejichž zveřejnění by samo o sobě mohlo ohrozit bezpečnost informačních systémů NNM. Dokument je proto určen k poskytování podle zákona č. 106/1999 Sb.

Pokud jsou součástí dokumentace k veřejné zakázce konkrétní technické konfigurace, provozní data, interní topologie, detailní logy, bezpečnostní nastavení nebo jiné citlivé informace, posuzuje jejich poskytování objednatel individuálně podle zákona č. 106/1999 Sb.

Takové informace mohou být neposkytnuty zejména tehdy, pokud by jejich zveřejnění mohlo ohrozit bezpečnost informačních a komunikačních systémů objednatele nebo usnadnit kybernetický útok, zejména podle § 11 odst. 1 písm. a) zákona č. 106/1999 Sb.; podle povahy věci mohou být dále chráněny též jako osobní údaje nebo obchodní tajemství.

Při posuzování poskytování informací objednatel zohlední rovněž povinnost zajištění kybernetické bezpečnosti podle zákona č. 264/2025 Sb., zejména povinnost předcházet zveřejnění informací, které by mohly zvýšit riziko kybernetického incidentu.

22. Specifické bezpečnostní požadavky podle typu systému

Není-li přístup, komunikace, integrace nebo oprávnění výslovně povoleno, považuje se za zakázané.

22.1 Obecná ustanovení pro specifické typy systémů

Pokud systém nesplňuje některý z požadavků této kapitoly, musí dodavatel tuto skutečnost doložit a navrhnout kompenzační bezpečnostní opatření.

Tyto požadavky doplňují obecná ustanovení tohoto dokumentu, přičemž v případě rozporu se použije přísnější požadavek a není-li stanoveno jinak, platí obecné požadavky v plném rozsahu i pro tyto systémy; dodavatel je povinen navrhnout řešení v souladu s těmito požadavky a řešení, které tyto požadavky nesplňuje, není přípustné.

Zařazení systému do konkrétní kategorie a aplikace těchto požadavků se provádí na základě charakteru systému a řízení rizik podle § 13 zákona č. 264/2025 Sb., přičemž rozhodující je posouzení objednatele.

Dodavatel je povinen uchovávat relevantní logy a technické záznamy po dobu stanovenou objednatelem nebo právními předpisy, minimálně však po dobu 6 měsíců, pokud není stanoveno jinak; skutečnost, že dodavatel označí požadavek za nesplnitelný nebo neaplikovatelný, nezbavuje dodavatele povinnosti tento stav řádně zdůvodnit a navrhnout adekvátní kompenzační bezpečnostní opatření.

22.2 Zařazení systému do kategorie

Zařazení systému do konkrétní kategorie podle této kapitoly provádí objednatel na základě charakteru systému, jeho funkcí, způsobu provozu a rizik pro ICT infrastrukturu a poskytování zdravotních služeb.

Dodavatel je povinen v nabídce uvést návrh zařazení systému a jeho odůvodnění, přičemž tento návrh nemá závazný charakter.

V případě pochybností nebo sporného zařazení rozhoduje objednatel. Dodavatel není oprávněn jednostranně určovat, že se na jím dodávané řešení nevztahují požadavky této kapitoly ani že spadá do méně přísné kategorie.

22.3 Vztah systémů k ICT infrastruktuře objednatele

Systémy nesmí být bez výslovného předchozího souhlasu objednatele připojeny do ICT infrastruktury objednatele, zejména do LAN/WAN sítě, domény, informačních systémů nebo sdílených služeb; pokud řešení vyžaduje nebo umožňuje napojení na ICT infrastrukturu objednatele, je dodavatel povinen tuto skutečnost jednoznačně uvést v nabídce a popsat rozsah, účel a způsob tohoto napojení, včetně veškerých komunikačních toků, používaných protokolů a požadavků na síťovou infrastrukturu.

Není přípustné navrhovat nebo realizovat řešení, která obsahují skryté, implicitní nebo nedokumentované napojení na ICT infrastrukturu objednatele, přičemž veškeré napojení podléhá schválení příslušného ICT útvaru objednatele.

Systém nesmí po instalaci automaticky navazovat komunikaci do externích sítí, cloudových služeb nebo na infrastrukturu dodavatele bez předchozího schválení objednatele, přičemž veškerá komunikace do externích sítí musí být výslovně definována, schválena objednatelem a omezena pouze na nezbytné cíle a služby.

Podmínky vzdáleného přístupu jsou dále specifikovány v kapitole 25.

22.4 Zdravotnické informační systémy (NIS, LIS, PACS, atd.)

Systém je považován za součást regulované služby ve zdravotnictví v režimu vyšších povinností a musí podporovat jednotnou autentizaci, řízení přístupů podle rolí a princip minimálních oprávnění, přičemž přístup k datům musí být řízen na úrovni rolí i jednotlivých oprávnění tak, aby byla zajištěna ochrana zdravotnické dokumentace.

Systém musí vést auditní logy zahrnující přístupy k dokumentaci, změny dat, exporty dat, administrátorské zásahy a chybové stavy, přičemž tyto logy musí být předávány do systému SIEM objednatele; dodavatel je povinen specifikovat rozsah a způsob zpracování osobních údajů a implementovaná technická a organizační opatření dle čl. 32 GDPR.

Musí být popsána všechna integrační rozhraní, datové toky a vazby na další systémy, včetně jejich bezpečnostního zajištění, přičemž systém musí být navržen s ohledem na vysokou dostupnost a provozní kontinuitu, včetně zajištění zálohování a obnovy dat, a musí umožňovat provoz v režimu vysoké dostupnosti odpovídající jeho kritičnosti.

Dodavatel je povinen popsat závislosti systému na dalších službách nebo dodavatelích; jakýkoliv vzdálený přístup musí být předem schválen objednatelem, auditovatelný a časově omezený.

22.5 Webové systémy / telemedicína

Dodavatel je povinen popsat architekturu řešení (on-premise / cloud / hybrid), způsob jeho provozu a vazby na další systémy, přičemž komunikace musí být šifrovaná a systém musí podporovat vícefaktorovou autentizaci pro přístup uživatelů i administrátorů; systém musí být navržen a provozován v souladu s bezpečnostními principy moderních webových aplikací, včetně ochrany proti běžným typům útoků (např. OWASP Top 10).

V případě veřejně dostupných systémů musí být zajištěna ochrana prostřednictvím bezpečnostních prvků, jako je reverzní proxy, WAF nebo obdobné technologie; dodavatel je povinen popsat všechna API rozhraní, způsob jejich zabezpečení, autentizace a řízení přístupů, přičemž API rozhraní musí být chráněna proti zneužití, zejména prostřednictvím omezení přístupu, autentizace a řízení objemu požadavků (rate limiting).

Datové toky musí být jednoznačně popsány, včetně přenosu osobních údajů, a v případě telemedicínských řešení musí být zajištěna ochrana zvláštní kategorie osobních údajů podle čl. 9 GDPR, zejména při jejich přenosu a ukládání.

Před nasazením systému musí být provedeno bezpečnostní testování (např. penetrační test nebo bezpečnostní audit) a odstranění zjištěných zranitelností, přičemž výsledky musí být na vyžádání předloženy objednateli; jakýkoliv vzdálený přístup musí být předem schválen objednatelem, auditovatelný a časově omezený.

22.6 Evakuační rozhlas / EPS / bezpečnostní OT systémy

Systém musí být navržen jako autonomní, funkčně samostatný systém nezávislý na ICT infrastruktuře NNM, přičemž jeho funkčnost nesmí být na této infrastruktuře závislá; systém nesmí být bez výslovného předchozího písemného souhlasu objednatele připojen do LAN/WAN infrastruktury nemocnice, do domény ani do jiných informačních systémů a jedinou přípustnou integrací je napojení na EPS nebo jiné bezpečnostní rozhraní výslovně uvedené v zadávací dokumentaci.

Pokud systém obsahuje IP nebo síťové prvky, je dodavatel povinen popsat architekturu, způsob komunikace, autentizace, logování a řízení přístupů, přičemž veškerá komunikace musí být řízena a omezena pouze na nezbytný rozsah; jakýkoliv vzdálený přístup musí být předem schválen objednatelem, auditovatelný, časově omezený a realizovaný bezpečným způsobem.

Systém musí být navržen tak, aby při výpadku napájení, sítě nebo řídicích prvků byla zachována jeho základní funkce v souladu s požadavky na evakuační systémy, nesmí být závislý na externích cloudových službách nebo internetové konektivitě, pokud to není výslovně schváleno objednatelem, a musí být provozovatelný i bez vzdáleného přístupu dodavatele a nesmí být závislý na výhradním přístupu dodavatele.

Součástí předání musí být kompletní technická dokumentace, aktuální konfigurace systému a administrátorské přístupy umožňující správu objednatelem nebo jím určenou třetí stranou.

22.7 MaR / BMS / SCADA / provozní OT systémy

Systémy měření a regulace (MaR), systémy řízení budov (BMS), SCADA systémy a obdobné provozní technologie musí být provozovány odděleně od běžné ICT infrastruktury objednatele a v režimu odpovídajícím provozním (OT) systémům; pokud systém vyžaduje síťovou komunikaci, musí být umístěn v přiřazeném síťovém segmentu (např. VLAN) odpovídajícím charakteru systému, který je logicky oddělen od běžné ICT infrastruktury objednatele, přičemž komunikace musí být řízena prostřednictvím síťových prvků, firewallu nebo nástrojů pro mikrosegmentaci a omezena pouze na nezbytný rozsah.

Systém nesmí být bez výslovného předchozího souhlasu objednatele integrován do domény, nemocničních informačních systémů ani sdílených ICT služeb; dodavatel je povinen v nabídce popsat architekturu systému, způsob komunikace, autentizace, řízení přístupů, logování a požadavky na síťovou infrastrukturu.

Jakýkoliv vzdálený přístup, zejména servisní přístup dodavatele, musí být předem schválen objednatelem, realizován bezpečným způsobem, auditovatelný a časově omezený; systém musí být navržen tak, aby minimalizoval závislost na externím připojení, umožňoval provoz i při omezení konektivity a neohrožoval dostupnost zdravotních služeb.

Systém musí být provozovatelný i bez vzdáleného přístupu dodavatele a nesmí být závislý na výhradním přístupu dodavatele; bezpečnostní opatření musí odpovídat charakteru OT systémů a nesmí narušit jejich bezpečný a spolehlivý provoz.

Součástí předání musí být kompletní technická dokumentace, aktuální konfigurace systému a administrátorské přístupy umožňující správu objednatelem nebo jím určenou třetí stranou.

22.8 Přístupové, docházkové a vjezdové systémy (ACS)

Přístupové, docházkové a vjezdové systémy musí být navrženy jako řízené systémy fyzické bezpečnosti s vazbou na identitní infrastrukturu objednatele, přičemž koncová zařízení musí být provozována ve přiřazeném síťovém segmentu (např. VLAN) a komunikace musí být řízena prostřednictvím firewallu nebo nástrojů pro mikrosegmentaci a omezena pouze na nezbytný rozsah v souladu s bezpečnostní politikou objednatele.

Centrální řídicí server může být provozován v ICT infrastruktuře objednatele, přičemž musí být zajištěno řízení přístupů, auditovatelnost a bezpečné oddělení od ostatních systémů; systém může být integrován na adresářové služby (např. AD) nebo systémy správy identit (IDM), přičemž oprávnění musí být řízena centrálně a v souladu s principem minimálních oprávnění.

Dodavatel je povinen popsat architekturu systému, způsob komunikace, autentizace, řízení přístupů a logování; jakýkoliv vzdálený přístup musí být předem schválen objednatelem, realizován bezpečným způsobem, auditovatelný a časově omezený.

Systém musí být provozovatelný i bez vzdáleného přístupu dodavatele a nesmí být závislý na výhradním přístupu dodavatele; musí umožnit jeho správu objednatelem nebo jím určenou třetí stranou a součástí předání musí být kompletní technická dokumentace, aktuální konfigurace systému a administrátorské přístupy.

22.9 Kamerové systémy (CCTV)

Kamerový systém musí být provozován v odděleném bezpečnostním režimu a ve přiřazeném nebo jinak logicky odděleném síťovém segmentu a nesmí být bez výslovného předchozího souhlasu objednatele integrován do jiných ICT systémů; musí být zajištěno řízení přístupů podle rolí a audit všech přístupů a exportů záznamů.

Dodavatel je povinen specifikovat způsob ukládání, dobu uchování (retenci) a ochranu záznamů v souladu s požadavky na ochranu osobních údajů, přičemž záznamy musí být chráněny proti neoprávněnému přístupu, kopírování nebo manipulaci a export záznamů musí být auditovatelný a umožněn pouze oprávněným uživatelům na základě řízení přístupů.

Jakýkoliv vzdálený přístup musí být předem schválen objednatelem, realizován bezpečným způsobem, řízený, auditovatelný a časově omezený, přičemž systém musí být provozovatelný i bez vzdáleného přístupu dodavatele a nesmí být závislý na výhradním přístupu dodavatele.

22.10 Zdravotnické prostředky připojené do infrastruktury objednatele (MD / IoMT)

Zdravotnické prostředky, které využívají síťovou komunikaci, zpracovávají data nebo jsou napojeny na ICT infrastrukturu objednatele (např. monitory životních funkcí, EKG, EEG, dávkovače, laboratorní analyzátory apod.), musí být posuzovány jako specifická kategorie systémů s omezenými možnostmi implementace standardních bezpečnostních opatření; tyto systémy zpravidla neumožňují plnou integraci do identitní infrastruktury, centralizovaného logování nebo

standardního řízení zranitelností, přičemž dodavatel je povinen tato omezení výslovně uvést a navrhnout odpovídající kompenzační bezpečnostní opatření.

Zdravotnické prostředky musí být provozovány v přiděleném síťovém segmentu odpovídajícím jejich charakteru (např. vyhrazená VLAN), přičemž komunikace musí být řízena a omezena pouze na nezbytné služby a systémy; není přípustné, aby zařízení vyžadovalo neomezený přístup do interní sítě objednatele nebo do internetu a veškerá komunikace musí být předem definována a schválena objednatelem.

Dodavatel je povinen uvést výrobce, model, verzi firmware a podporovanou dobu životního cyklu zařízení.

Dodavatel je povinen poskytnout informace o způsobu zabezpečení zařízení, zejména o podpoře aktualizací, řízení zranitelností, autentizaci a řízení přístupů, včetně uvedení omezení z hlediska kybernetické bezpečnosti; v případě, že zařízení neumožňuje implementaci některých požadavků tohoto dokumentu, musí být tato omezení kompenzována vhodnými opatřeními na úrovni infrastruktury objednatele (např. segmentace, firewall, monitoring komunikace).

Zařazení zařízení do této kategorie a stanovení konkrétních bezpečnostních opatření provádí objednatel na základě posouzení rizik.

22.11 Běžné ICT systémy

Běžnými ICT systémy se pro účely tohoto dokumentu rozumí systémy, které nejsou zařazeny do specifických kategorií dle této kapitoly, zejména zdravotnické systémy, webové a telemedicínské systémy, bezpečnostní OT systémy, systémy fyzické bezpečnosti nebo systémy řízení budov; typicky se jedná o administrativní a podpůrné systémy, koncová zařízení, serverové aplikace, databázové systémy, integrační nástroje, middleware, tiskové systémy, kancelářské aplikace, pomocné provozní systémy a další ICT komponenty provozované v rámci standardní infrastruktury objednatele, na které se plně použijí obecné požadavky tohoto dokumentu.

Dodavatel je povinen popsat architekturu řešení, datové toky, integrace na další systémy, způsob autentizace, řízení přístupů a logování, přičemž zařazení systému do této kategorie provádí objednatel na základě posouzení rizik a návrh dodavatele má nezávazný charakter.

Tato kategorie nesmí být využívána k obcházení přísnějších požadavků stanovených pro jiné typy systémů; posouzení správnosti zařazení systému provádí objednatel a v případě nejasností ohledně zařazení systému do této nebo jiné kategorie rozhoduje objednatel.

22.12 Integrace mezi systémy

Integrace mezi systémy musí být navržena a realizována tak, aby nedocházelo k neřízenému propojení systémů ani k nepřiměřenému rozšiřování bezpečnostního perimetru, přičemž každá integrace musí být jednoznačně popsána z hlediska architektury, datových toků, přenášených dat a bezpečnostních opatření; dodavatel je povinen popsat všechna integrační rozhraní, včetně použitých protokolů, způsobu autentizace, autorizace a řízení přístupů.

Integrace musí být realizována s využitím zabezpečené komunikace a principu minimálních oprávnění a nesmí docházet k přímému sdílení databází ani k obcházení aplikační logiky systémů, pokud to není výslovně schváleno objednatelem na základě posouzení rizik; integrace mezi systémy musí být logicky oddělena prostřednictvím síťových prvků, firewallu nebo nástrojů pro mikrosegmentaci, zejména pokud propojuje systémy s rozdílnou úrovní kritičnosti nebo bezpečnostního režimu.

V případě integrace se systémy třetích stran nebo externími službami (včetně cloudových služeb) je dodavatel povinen popsat způsob zabezpečení komunikace, umístění dat, odpovědnosti jednotlivých subjektů a případné přeshraniční přenosy dat, přičemž integrace musí být navržena tak, aby bylo možné ji nezávisle měnit nebo nahradit bez zásahu do ostatních systémů a nesmí vytvářet závislost na výhradním řešení dodavatele (vendor lock-in); musí umožňovat správu, monitoring a audit objednatelem nebo jím určenou třetí stranou.

Veškeré integrační operace, včetně přístupů k rozhraním a přenosů dat, musí být auditovatelné a zaznamenávané v logovacím systému objednatele nebo musí být umožněno jejich předání do tohoto systému; každá integrace podléhá předchozímu schválení objednatelem na základě posouzení rizik.

Není přípustné navrhovat nebo realizovat integrace do ICT infrastruktury objednatele, které nejsou výslovně popsány v nabídce, projektové dokumentaci nebo technické specifikaci a schváleny objednatelem; integrace nesmí vytvářet nepřiměřené bezpečnostní riziko ani obcházet bezpečnostní architekturu objednatele a jakákoli nepopsaná nebo neschválená integrace je nepřípustná.

23. Referenční architektura a používané technologie ICT prostředí objednatele

Objednatel využívá standardizovanou ICT architekturu založenou na definovaných technologických principech a konkrétních technologiích, které musí být dodavatelem respektovány a zohledněny při návrhu, implementaci a provozu dodávaného řešení. Tento výčet představuje standardní technologické prostředí objednatele, které musí být dodavatelem respektováno a zohledněno při návrhu řešení.

Uvedené technologie představují standardní prostředí objednatele; dodavatel není povinen tyto technologie dodávat, ale musí zajistit kompatibilitu s nimi.

Není přípustné navrhovat řešení, které vyžaduje obcházení, deaktivaci nebo nahrazení těchto technologií, pokud objednatel nestanoví jinak.

V prostředí objednatele jsou využívány zejména následující technologie a systémy:

síťová infrastruktura:	Aruba (switche, bezdrátová infrastruktura),
řízení přístupu do sítě:	Aruba ClearPass (NAC),
bezpečnost perimetru a komunikace:	Check Point (firewall),
monitoring a dohled nad provozem:	Flowmon, PRTG,
správa identit a přístupů:	Active Directory, IDM,
logování a bezpečnostní monitoring:	Elastic (SIEM),
virtualizační platforma:	VMware,
úložiště dat:	Qumulo.

Dodavatel je povinen navrhnout řešení tak, aby bylo s uvedenými technologiemi kompatibilní, umožňovalo jejich využití v rozsahu odpovídajícím charakteru systému a nevyžadovalo jejich obcházení, deaktivaci, nahrazení nebo zásadní změnu architektury prostředí objednatele.

Řešení musí být navrženo tak, aby umožňovalo integraci do existující infrastruktury objednatele, zejména v oblasti autentizace, řízení přístupů, logování, monitoringu a síťové komunikace, pokud to povaha systému umožňuje nebo pokud objednatel nestanoví jinak.

Konkrétní technická implementace, konfigurace, topologie sítě a detailní architektura prostředí objednatele nejsou součástí tohoto dokumentu a mohou být sděleny pouze v rámci konkrétní veřejné zakázky nebo jiné neveřejné dokumentace objednatele.

24. Specifické bezpečnostní požadavky objednatele (včetně požadavků zřizovatele)

Tato kapitola doplňuje obecné a technické požadavky dokumentu o konkrétní provozní a bezpečnostní pravidla; v případě rozporu se použije přísnější požadavek.

24.1 Obecná ustanovení

Objednatel stanovuje specifické bezpečnostní a provozní požadavky, které vycházejí z jeho interních pravidel a současně zohledňují požadavky zřizovatele (Kraje Vysočina), relevantní legislativu a principy řízení kybernetické bezpečnosti; tyto požadavky jsou pro dodavatele závazné v plném rozsahu a doplňují obecná ustanovení tohoto dokumentu, přičemž v případě rozporu se použije přísnější požadavek.

24.2 Identita, autentizace a správa přístupů

Dodavatel je povinen zajistit ochranu přístupových údajů a používat výhradně personifikované účty jednoznačně přiřaditelné ke konkrétní fyzické osobě; přístupová oprávnění mohou být využívána pouze pro schválený účel a v rozsahu odpovídajícím principu minimálních oprávnění.

Autentizace musí odpovídat aktuálním bezpečnostním standardům, zejména s využitím vícefaktorové autentizace tam, kde to povaha systému umožňuje (zejména vzdálený přístup, privilegované účty a přístup k citlivým systémům).

Hesla musí být chráněna proti neoprávněnému zpřístupnění, ukládána výhradně v zabezpečené (hashované) podobě a nesmí obsahovat odvoditelné informace (např. jméno, login nebo název organizace); v případě podezření na kompromitaci musí být neprodleně změněna.

Minimální požadavky na hesla jsou stanoveny dle bezpečnostní politiky objednatele následovně:

běžné uživatelské účty:

- minimální délka 12 znaků,
- obsah čtyř kategorií znaků (malá písmena, velká písmena, číslice, speciální znaky)

privilegované (administrátorské) účty:

- minimální délka 20 znaků,
- obsah čtyř kategorií znaků (malá písmena, velká písmena, číslice, speciální znaky)
- povinné použití vícefaktorové autentizace, pokud to technicky umožňuje způsob přístupu.

účty externích dodavatelů:

- minimální délka 17 znaků,
- obsah čtyř kategorií znaků (malá písmena, velká písmena, číslice, speciální znaky)
- povinné použití vícefaktorové autentizace, pokud to technicky umožňuje způsob přístupu.

Platnost hesel je omezena na maximálně 12 měsíců, přičemž změna hesla musí být provedena vždy při podezření na jeho kompromitaci nebo při změně oprávnění.

Objednatel využívá centralizovanou správu identit a přístupů (IDM), která může u vybraných typů účtů uplatňovat odlišná pravidla než doménová politika Active Directory; dodavatel je povinen tyto rozdíly respektovat a řídit se pravidly stanovenými objednatelem.

Privilegované účty musí být odděleny od běžných uživatelských účtů a jejich použití musí být omezeno výhradně na činnosti správy a údržby systému; veškeré použití těchto účtů musí být auditovatelné.

Přístupová oprávnění třetích stran podléhají schválení objednatelem a musí být časově omezená, pravidelně přezkoumávaná a neprodleně odebrána po ukončení důvodu jejich přidělení.

24.3 Součinnost a řízení změn

Dodavatel je povinen zajistit součinnost s ICT útvarem objednatele při návrhu, implementaci a provozu řešení, přičemž veškeré zásahy do infrastruktury, změny konfigurace a integrační kroky podléhají předchozímu schválení objednatelem a musí být oznámeny s dostatečným předstihem. Dodavatel je současně povinen respektovat požadavky na evidenci a řízení změn, včetně vedení dokumentace v nástroji určeném objednatelem nebo zřizovatelem (např. Technet), pokud objednatel nestanoví jinak.

24.4 Vzdálený přístup

Vzdálený přístup dodavatele do ICT infrastruktury objednatele je povolen pouze na základě předchozího schválení objednatele, v rozsahu a po dobu nezbytně nutnou pro plnění smluvních povinností. Přístup musí být řízený, auditovatelný a nesmí být využíván mimo schválený účel. Podrobné podmínky vzdáleného přístupu jsou stanoveny v samostatné kapitole 25.

24.5 Řízení rizik, bezpečný provoz a vývoj

Dodavatel je povinen zajistit řízení rizik v rozsahu odpovídajícím charakteru plnění, zejména identifikaci aktiv, hodnocení rizik a jejich průběžné řízení. Současně je povinen zajistit bezpečný vývoj a provoz řešení, včetně ochrany zdrojových kódů, řízení přístupů, verzování, logování a zálohování, a nesmí zaznamenávat citlivé údaje (např. hesla nebo kryptografické klíče) do logů.

24.6 Řízení bezpečnostních incidentů

Dodavatel je povinen bez zbytečného odkladu informovat objednatele o bezpečnostních incidentech nebo nestandardním chování souvisejícím s informačními aktivy objednatele a poskytnout součinnost při jejich řešení, včetně analýzy a plnění oznamovacích povinností.

24.7 Kryptografie a ochrana komunikace

Používané kryptografické prostředky musí odpovídat aktuálním doporučením NÚKIB a nesmí využívat zastaralé nebo nedostatečně bezpečné algoritmy; komunikace musí být šifrována s využitím standardních protokolů (např. TLS 1.2 a vyšší) a bezpečných konfigurací.

24.8 Vztah k požadavkům zřizovatele

Dodavatel je povinen zohlednit také další bezpečnostní a provozní požadavky vyplývající z metodik a pokynů zřizovatele, pokud jsou objednatelem aplikovány; není přípustné jejich obcházení nebo snižování jejich úrovně. Podrobnější podmínky mohou být stanoveny samostatnou přílohou nebo provozní dokumentací objednatele.

25. Vzdálený přístup

Dodavatel je povinen při návrhu řešení zohlednit, že veškerý vzdálený přístup bude realizován výhradně v souladu s touto kapitolou.

25.1 Obecná ustanovení

Vzdálený přístup do ICT infrastruktury objednatele je umožněn pouze v případech, kdy je nezbytný pro plnění smluvních, servisních nebo provozních činností dodavatele, a to vždy na základě předchozího schválení objednatelem. Dodavatel je povinen navrhovat řešení tak, aby potřeba vzdáleného přístupu byla minimalizována a aby systém nebyl závislý na trvalém vzdáleném přístupu dodavatele.

Veškeré vzdálené přístupy musí být řízené, auditovatelné, časově omezené a jednoznačně přiřaditelné ke konkrétní fyzické osobě; není přípustné využívání sdílených účtů ani neřízených přístupů. Přístup smí být využíván výhradně pro schválený účel a v rozsahu odpovídajícím principu minimálních oprávnění.

25.2 Způsob realizace vzdáleného přístupu

Primárním způsobem realizace vzdáleného přístupu je zabezpečené připojení prostřednictvím VPN infrastruktury objednatele provozované na bezpečnostní platformě Check Point, přičemž komunikace probíhá primárně v IPv4 a podpůrně v IPv6. Přístup je chráněn vícefaktorovou autentizací.

Po navázání VPN spojení je přístup omezen bezpečnostními pravidly pouze na určené systémy, síťové segmenty a nezbytné služby; není přípustné požadovat plošný nebo neomezený přístup do infrastruktury objednatele. Veškerá komunikace podléhá řízení, filtrování a logování.

Vedle plného síťového přístupu může objednatel umožnit přístup k vybraným aplikacím prostřednictvím aplikačního nebo portálového řešení, které omezuje rozsah dostupných služeb pouze na konkrétní publikované aplikace.

25.3 Propojení systémů (IPsec, neveřejné sítě)

V odůvodněných případech může být realizováno trvalé propojení mezi infrastrukturou objednatele a infrastrukturou dodavatele formou šifrovaného IPsec tunelu, zpravidla navazovaného z prostředí objednatele směrem k dodavateli. Takové propojení podléhá individuálnímu schválení a musí být omezeno pouze na konkrétní definované komunikační toky.

Dodavatel je povinen předem doložit technický popis komunikace, zejména cílové adresy, porty, protokoly a účel komunikace. Není přípustné požadovat obecný nebo neomezený síťový přístup.

25.4 Výjimečné přístupy a operativní zásahy

Ve výjimečných případech může být povolen jiný způsob vzdáleného přístupu (např. přímé připojení na službu nebo nástroj vzdálené podpory), vždy však pouze na základě předchozího schválení, na omezenou dobu a pro konkrétní účel. Tyto přístupy jsou standardně blokovány a jejich povolení je realizováno pouze dočasně.

25.5 Žádosti o vzdálený přístup a lhůty

Požadavky na zřízení, změnu nebo zrušení vzdáleného přístupu je dodavatel povinen zasílat prostřednictvím oficiálního kontaktního e-mailu ICT útvaru objednatele: it@nnm.cz, pokud objednatel nestanoví jinak.

Žádost musí být podána minimálně 3 pracovní dny předem, pokud není dohodnuto jinak, a musí obsahovat minimálně:

jméno a příjmení osoby, e-mailovou adresu, mobilní telefonní číslo (pro účely vícefaktorového ověření), název organizace dodavatele, důvod požadavku, požadovaný rozsah oprávnění (systémy, služby), požadované časové období přístupu.

V případě plánovaných servisních zásahů je dodavatel povinen oznámit termín a rozsah prací minimálně 2 pracovní dny předem. V případě mimořádných nebo havarijních situací lze tyto lhůty přiměřeně zkrátit, avšak přístup musí být vždy dodatečně evidován a schválen.

Neúplné žádosti mohou být odmítnuty nebo vráceny k doplnění.

25.6 Provozní pravidla a omezení

Jakýkoliv vzdálený přístup musí být předem schválen objednatelem, časově omezen a po ukončení činnosti ukončen. Dodavatel je povinen zajistit, že osoby využívající přístup budou jednoznačně identifikovatelné a budou jednat v souladu s bezpečnostní politikou objednatele.

Objednatel si vyhrazuje právo vzdálený přístup kdykoliv omezit, přerušit nebo ukončit, zejména v případě bezpečnostního incidentu nebo porušení pravidel.

25.7 Bezpečnostní omezení

Objednatel aktivně blokuje neautorizované nástroje pro vzdálený přístup a monitoruje pokusy o jejich použití. Dodavatel není oprávněn používat vlastní VPN řešení, tunelování ani jiné prostředky pro obcházení bezpečnostních opatření objednatele.

Dodavatel je povinen zajistit, aby všechny osoby využívající vzdálený přístup byly prokazatelně poučeny o těchto pravidlech a dodržovaly je.