PORTÁL NÚKIB

Požadavky na bezpečnostní role

TLP:CLEAR

21. dubna 2026

Verze 1.1

Národní úřad
pro kybernetickou
a informační bezpečnost

1 Co se dozvím v tomto dokumentu?

Tento dokument obsahuje popis závazných a doporučujících požadavků na výbor pro řízení kybernetické bezpečnosti a pro jednotlivé bezpečnostní role (manažer, architekt, auditor kybernetické bezpečnosti a garant aktiva). Materiál je určen pro poskytovatele regulovaných služeb v režimu vyšších povinností.

Pokud máte jakékoliv další otázky, podívejte se na www.portal.nukib.gov.cz nebo nám napište na regulace@nukib.gov.cz.

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti publikované verze dokumentu.

2 Závazné a doporučující požadavky na bezpečnostní role

Závazné požadavky na výkon jednotlivých bezpečnostních rolí mohou vyplývat pouze ze zákona č. 264/2025 Sb., o kybernetické bezpečnosti, a z jeho prováděcích předpisů, zejména vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (dále jen „vyhláška č. 409/2025 Sb.“). U požadavků se taktéž aplikuje § 3 písm. c) vyhlášky č. 409/2025 Sb., dle kterého *„povinná osoba* […] *zavede a provádí přiměřená bezpečnostní opatření směřující k zajištění kybernetické bezpečnosti regulované služby na základě cílů systému řízení bezpečnosti informací, bezpečnostních potřeb a řízení rizik“*.

V rámci řízení rizik je možné, že bude výkonem bezpečnostní role pověřena osoba, která závazné požadavky plní pouze částečně. Pověření takové osoby musí být řádně zdůvodněno v rámci prohlášení o aplikovatelnosti, resp. v rámci řízení rizik.

Doporučené požadavky nemají závazný charakter a kopírují nejlepší praxi v této oblasti. Poskytovatelé regulovaných služeb samozřejmě mohou požadovat splnění dalších podrobnějších či striktnějších požadavků, například delší praxi, specifickou certifikaci či zkušenosti z konkrétních projektů.

Osoby jmenované poskytovatelem regulované služby do funkce jednotlivých bezpečnostních rolí **nemusí být vůči poskytovateli regulované služby v zaměstnaneckém či obdobném poměru**. Bezpečnostní role mohou být vykonávány také externisty.

Vrcholné vedení má povinnost zajistit **zastupitelnost** manažera a architekta kybernetické bezpečnosti (§ 4 odst. 5 vyhlášky č. 409/2025 Sb.). Pro zajištění zastupitelnosti je možné dočasné rozložení povinností a kompetencí mezi více osob.

3 Výbor pro řízení kybernetické bezpečnosti

Podle § 4 odst. 3 vyhlášky č. 409/2025 Sb.:

Vrcholné vedení zřídí výbor pro řízení kybernetické bezpečnosti *a určí jeho členy, přičemž*

a) *zajistí, že členem výboru pro řízení kybernetické bezpečnosti bude alespoň 1 člen vrcholného vedení nebo jím pověřená osoba a manažer kybernetické bezpečnosti,*
b) *určí práva a povinnosti výboru pro řízení kybernetické bezpečnosti a jeho členů, související se systémem řízení bezpečnosti informací,*
c) *zajistí konání pravidelných jednání výboru pro řízení kybernetické bezpečnosti alespoň jednou ročně,*
d) *zajistí vyhotovení záznamu o průběhu jednání výboru pro řízení kybernetické bezpečnosti a*
e) *zajistí, že výbor pro řízení kybernetické bezpečnosti je složen z osob s pravomocemi a odbornou způsobilostí pro celkové řízení a rozvoj systému řízení bezpečnosti informací a osob významně se podílejících na řízení a koordinaci činností spojených s*

Výbor pro řízení kybernetické bezpečnosti je organizovaná skupina tvořená osobami, které jsou pověřeny celkovým řízením a rozvojem regulované služby anebo se významně podílejí na řízení a koordinaci činností spojených s kybernetickou bezpečností regulované služby.

V praxi může být výbor pro řízení kybernetické bezpečnosti tvořen lidmi z vrcholového i středního managementu, zároveň by měl mít většinu zástupců z oblasti ICT a bezpečnosti (může se lišit podle způsobu řízení jednotlivých organizací). Konkrétní způsob sestavení výboru pro řízení kybernetické bezpečnosti je plně v rukou vedení organizace, nový zákon o kybernetické bezpečnosti ani jeho prováděcí právní předpisy jej nad rámec výše uvedeného neregulují.

Klíčové činnosti	a) Celkové řízení a rozvoj kybernetické bezpečnosti v rámci povinné osoby. b) Tvorba rámce kybernetické bezpečnosti, směrování a zásad kybernetické bezpečnosti povinné osoby (definování strategických cílů a směrování rozvoje v oblasti kybernetické bezpečnosti). c) Definice rolí a odpovědností v rámci systému řízení bezpečnosti informací. d) Definice požadavků na podávání zpráv a kontrolu systému řízení bezpečnosti informací. e) Kontrola aktuálního stavu kybernetické bezpečnosti v rámci povinné osoby a zjišťování, zda dochází k naplňování plánovaných cílů.

4 Manažer kybernetické bezpečnosti

Podle § 5 odst. 1 vyhlášky č. 409/2025 Sb.:

*Je pověřen řízením systému řízení bezpečnosti informací, přičemž výkonem této role může být pověřena osoba, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost **praxí s řízením kybernetické bezpečnosti nebo s řízením bezpečnosti informací po dobu alespoň 3 let**.*

Odpovídá za pravidelné informování vrcholného vedení o činnostech vyplývajících z rozsahu jeho odpovědnosti a stavu systému řízení bezpečnosti informací.

Nesmí být pověřen výkonem rolí odpovědných za provoz technických aktiv regulované služby.

Manažer kybernetické bezpečnosti je zodpovědný za pravidelné informování vrcholného vedení o činnostech, které vyplývají z rozsahu jeho odpovědnosti a stavu systému řízení informační bezpečnosti.

V praxi je manažer kybernetické bezpečnosti jakýmsi mezistupněm mezi vrcholným vedením a operativní úrovní. Výkon role manažera kybernetické bezpečnosti musí být oddělen od rolí, které jsou odpovědné za provoz technických aktiv regulované služby. Pro správný výkon této role je zapotřebí zajistit potřebné pravomoci, odpovědnosti a finanční zdroje.

4.1 Doporučené požadavky

Klíčové činnosti	a) Řízení systému bezpečnosti informací. b) Pravidelné informování vrcholného vedení povinné osoby. c) Pravidelná komunikace s vrcholným vedením povinné osoby. d) Koordinace a podílení se na procesu řízení aktiv a rizik. e) Předkládání zpráv o hodnocení aktiv a rizik, plánu zvládání rizik a prohlášení o aplikovatelnosti na jednání výboru pro řízení kybernetické bezpečnosti. f) Poskytování pokynů pro zajištění bezpečnosti informací při sjednání, hodnocení, výběru, řízení a ukončení dodavatelských vztahů. g) Komunikace s Vládním nebo Národním CERT. h) Koordinace řízení incidentů. i) Vyhodnocování vhodnosti a účinnosti bezpečnostních opatření.
Znalosti	a) Normy řady ISO/IEC 27000 a obdobné normy z oblasti bezpečnosti a ICT.

	b) Přehled v oblasti ICT (operační systémy, databáze, aplikace, datové sítě) s důrazem na bezpečnost. c) Řízení rizik. d) Řízení kontinuity činností. e) Relevantní právní a regulatorní požadavky, zejména zákona. f) Kontext povinné osoby.
Zkušenosti	a) Prosazování systému řízení bezpečnosti informací. b) Porozumění definicím rizik a rizikovým scénářům. c) Řízení rizik v rámci povinné osoby. d) Schopnost interpretovat výsledky řízení rizik a koordinovat zvládání rizik.
Relevantní certifikace	a) Certified Information Security Manager (CISM), b) Certified in Risk and Information Systems Control (CRISC), c) Certified Information Systems Security Professional (CISSP), d) Manažer BI (akreditační schéma ČIA). Případně jiná certifikace dokládající odbornou způsobilost vydána certifikačním orgánem certifikujícím osoby v souladu s požadavky normy ČSN EN ISO/IEC 17024.

5 Architekt kybernetické bezpečnosti

Podle § 5 odst. 2 vyhlášky č. 409/2025 Sb.:

Je pověřen k zajištění návrhu implementace bezpečnostních opatření tak, aby byla zajištěna bezpečná architektura regulované služby, přičemž výkonem této role může být pověřena osoba, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost ***praxí s navrhováním implementace bezpečnostních opatření a zajišťováním bezpečné architektury v délce alespoň 3 let.***

V praxi je architekt kybernetické bezpečnosti odpovědný za návrh bezpečnostní architektury od komunikační infrastruktury, až například po bezpečnost na aplikační úrovni. Rovněž odpovídá za následnou implementaci navržených bezpečnostních opatření.

5.1 Doporučené požadavky

Klíčové činnosti	a) Odpovědnost za návrh implementace bezpečnostních opatření. b) Odpovědnost za stanovení, dokumentování, údržbu a neustálý rozvoj vhodné bezpečné architektury regulované služby podle aktuální dobré praxe.
Znalosti	a) Architektura informačních a komunikačních systémů a její navrhování. b) Hardwarové komponenty, nástroje a architektury. c) Operační systémy a software. d) Podnikové procesy a jejich integrace a závislost na ICT. e) Řízení bezpečnosti a rizik. f) Bezpečnost komunikací a sítí. g) Řízení identit a přístupů. h) Hodnocení a testování bezpečnosti. i) Bezpečnost provozu. j) Základní principy bezpečného vývoje softwaru. k) Integrace a závislosti ICT a obchodních procesů.
Zkušenosti	a) Navrhování implementace bezpečnostních opatření. b) Navrhování bezpečné architektury. c) Bezpečnost vývoje softwaru.
Relevantní certifikace	a) Certified Information Security Manager (CISM), b) Certified in Risk and Information Systems Control (CRISC), c) Certified Information Systems Security Professional (CISSP), d) Manažer BI (akreditační schéma ČIA). Případně jiná certifikace dokládající odbornou způsobilost vydána certifikačním orgánem certifikujícím osoby v souladu s požadavky normy ČSN EN ISO/IEC 17024.

6 Auditor kybernetické bezpečnosti

Podle § 5 odst. 4 vyhlášky č. 409/2025 Sb.:

Je pověřen prováděním auditu kybernetické bezpečnosti, přičemž výkonem této role může být pověřena osoba, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost ***praxí s prováděním auditů kybernetické bezpečnosti nebo auditů systému řízení bezpečnosti informací v délce alespoň 3 let.***

Zaručuje, že provedení auditu kybernetické bezpečnosti je nestranné.

Nesmí být pověřen výkonem jiných bezpečnostních rolí.

Úlohou auditora kybernetické bezpečnosti je posouzení míry souladu systému řízení bezpečnosti informací a implementovaných bezpečnostních opatření s právními předpisy, vnitřními předpisy, smluvními závazky a nejlepší praxí.

6.1 Doporučené požadavky

Klíčové činnosti	a) Provádění auditu kybernetické bezpečnosti. b) Hodnocení správnosti a účinnosti zavedených bezpečnostních opatření.
Znalosti	a) Metodologie a rámce auditu informační bezpečnosti. b) Procesy a postupy interního auditu. c) Role a funkce interního auditu. d) Proces provádění auditu ICT bezpečnosti. e) Strategické a taktické řízení ICT. f) Akvizice, vývoj a nasazení ICT. g) Řízení provozu, údržby a služeb ICT. h) Ochrana aktiv. i) Hodnocení kybernetické bezpečnosti, metody testování a vzorkování. j) Relevantní právní předpisy. k) ICT bezpečnost.
Zkušenosti	a) Plánování auditů informační nebo kybernetické bezpečnosti. b) Provádění auditů kybernetické bezpečnosti nebo auditů systému řízení bezpečnosti informací. c) Analyzování výsledků auditů.

	d) Psaní auditních závěrů, jejich prezentace a navrhování doporučení vedoucích k nápravě nálezů. e) Reporting stavu plnění zákonných požadavků. f) Provádění auditů se zaměřením na ICT a informační nebo kybernetickou bezpečnost.
Relevantní certifikace	a) Certified Information Systems Auditor (CISA), b) Certified Internal Auditor (CIA), c) ISO/IEC 27001 Lead Auditor, d) Auditor BI (akreditační schéma ČIA). Případně jiná certifikace dokládající odbornou způsobilost vydána certifikačním orgánem certifikujícím osoby v souladu s požadavky normy ČSN EN ISO/IEC 17024.

7 Garant aktiva

Podle § 5 odst. 3 vyhlášky č. 409/2025 Sb.
Je pověřen k zajištění rozvoje, použití a bezpečnost aktiva.

Garant aktiva má za úkol zajistit důvěrnost, integritu a dostupnost daného aktiva, a také se podílet na určení a hodnocení rizik.

V normách řady ISO/IEC 27000 se využívá pojem vlastník aktiva, ale v praxi se jedná o tutéž roli.

7.1 Doporučené požadavky

Klíčové činnosti	a) Zajištění rozvoje, použití a bezpečnosti aktiva. b) Spolupráce s ostatními osobami zastávajícími bezpečnostní role. c) Provádění určování a hodnocení aktiv a rizik.
Znalosti	a) Dobrá znalost aktiva, jehož je garantem. b) Dobrá znalost interních bezpečnostních politik a metodik (například metodiky pro hodnocení aktiv a rizik).

8 Časté dotazy a odpovědi ohledně bezpečnostních rolí

1. **Co když mám vyškolenou osobu, kterou chci dosadit do bezpečnostní role, ale ta nesplňuje požadavky na požadovanou délku praxe?**

V případě, že osoba jmenovaná do bezpečnostní role nesplňuje požadovanou délku praxe, je nutné zohlednit tuto skutečnost v rámci řízení rizik podle § 8 vyhlášky č. 409/2025 Sb., kde je možné příslušné riziko řídit a formou prohlášení o aplikovatelnosti patřičně odůvodnit nenaplnění konkrétního požadavku vyhlášky. Tímto řešením by však nemělo docházet k záměrnému obcházení požadavků vyhlášky, aniž by se poskytovatel regulované služby pokusil požadavky řádně splnit (např. najít vhodnou osobu k obsazení dané bezpečnostní role).

2. **Je možné pro zajištění bezpečnostní role najmout externího pracovníka, tj. bezpečnostní roli „outsourcovat“?**

Ve vyhlášce č. 409/2025 Sb. není zakotvena povinnost výkonu bezpečnostní role interním zaměstnancem.

V případě zajištění bezpečnostní role externí osobou je před uzavřením smlouvy vhodné ošetřit požadavky na vzdělání a certifikaci ve smlouvě. Taktéž existují další požadavky vyhlášky č. 409/2025 Sb. na řízení dodavatelů. Je na poskytovateli regulované služby, zda si určí, že bezpečnostní rizika plynoucí z externího zajištění bezpečnostní role jsou pro ni přijatelná či nikoliv.

V případě zajištění několika bezpečnostních rolí jedním dodavatelem je nutné také zohlednit možné riziko střetu zájmů. Především u role auditora kybernetické bezpečnosti totiž hrozí nedodržení požadavku na provedení nestranného auditu kybernetické bezpečnosti.

3. **Může jedna osoba zajišťovat více bezpečnostních rolí současně?**

Dle vyhlášky č. 409/2025 Sb. nesmí být osoba pověřená výkonem bezpečnostní role manažera kybernetické bezpečnosti pověřena výkonem rolí odpovědných za provoz technických aktiv regulované služby.

Dále nesmí být osoba pověřená výkonem bezpečnostní role auditora kybernetické bezpečnosti pověřena výkonem jiných bezpečnostních rolí, tj. manažerem kybernetické bezpečnosti, architektem kybernetické bezpečnosti nebo garantem aktiva. U ostatních rolí není stanovena žádná jiná podmínka o nemožnosti výkonu jiných bezpečnostních rolí.

4. **Jak prokazovat požadovanou délku praxe?**

Prokazování praxe není ve vyhlášce č. 409/2025 Sb. nijak definováno. Cílem však je, aby bezpečnostní role vykonávaly osoby způsobilé. Je tedy na uvážení poskytovatele regulované služby, jakým způsobem bude k této problematice přistupovat.

5. **Může manažera kybernetické bezpečnosti zastupovat například bezpečnostní ředitel?**

Je nutné zvážit požadavky stanovené na bezpečnostní roli manažera kybernetické bezpečnosti. Požadavky na odbornost a praxi je možné při zajištění zastupitelnosti manažera kybernetické

bezpečnosti uplatnit přiměřeně, přičemž zastupování lze rozdělit mezi více osob podle konkrétních povinností a kompetencí manažera kybernetické bezpečnosti.

Dále se považuje za vhodné, aby určený zástup nebyl současně odpovědný za provoz technických aktiv regulované služby. Rovněž zde je možné přistupovat přiměřeně, s ohledem na organizační strukturu a personální možnosti poskytovatele regulované služby, přičemž volba zástupu musí být vždy smysluplná a odpovídat bezpečnostním potřebám poskytovatele regulované služby.

9 Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol. Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
TLP:RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
TLP:AMBER+STRICT	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:AMBER	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:GREEN	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
TLP:CLEAR	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Verze dokumentu			
datum	**verze**	**změněno**	**popis změny**
8. prosince 2025	1.0	OREG + OK	Vytvoření dokumentu
21. dubna 2026	1.1	OK	Oprava certifikací u auditora KB