# Příloha RD03 - Práva a povinnosti manažera a architekta kybernetické bezpečnosti ISÚI a RÚIAN

č. sml. Objednatele: ČÚZK-52271/2023

č. sml. Zhotovitele: CZBAP-2245

# Obsah

# 1. Úvod

Práva a povinnosti manažera a architekta kybernetické bezpečnosti uvedené v tomto dokumentu se týkají Rámcové dohody na Rozvoj a údržbu Informačního systému (IS) registru územní identifikace, adres a nemovitostí, IS územní identifikace a IS veřejného dálkového přístupu v letech 2024 –2027.

# 2. Práva a povinnosti manažera kybernetické bezpečnosti IS

Manažer kybernetické bezpečnosti IS zajišťuje systém řízení bezpečnosti informací pro daný IS, a odpovídá se manažeru kybernetické bezpečnosti ČÚZK.

Zastupování osoby určené do bezpečnostní role zajištěné dodavatelem musí být zajištěno smluvně.

Povinnosti manažera kybernetické bezpečnosti IS jsou:

- znalost ZoKB, jeho prováděcích vyhlášek a souvisejících předpisů,
- zajistit bezpečnost primárních aktiv v rámci daného IS KII nebo VIS, tj. jejich důvěrnosti, dostupnosti a integrity,
- neprodleně hlásit kybernetické bezpečnostní incidenty IS KII/VIS manažerovi kybernetické bezpečnosti ČÚZK, a vést jejich evidenci,
- připravovat pro manažera kybernetické bezpečnosti ČÚZK podklady pro NÚKIB,
- připravovat za IS KII/VIS pro manažera kybernetické bezpečnosti ČÚZK podklady pro jednání VŘKB,
- spolupracovat na odstranění nedostatků zjištěných při kontrolách NÚKIB,
- zajišťovat provedení reaktivních opatření,
- poskytovat součinnost auditorovi kybernetické bezpečnosti a auditorům KÚ/ZÚ/ČÚZK při provádění auditů a kontrol,
- vyhodnocovat a klasifikovat kybernetický bezpečnostní incident, prošetřovat a určovat jeho příčiny, a dokumentovat zvládání kybernetických bezpečnostních incidentů,
- vyhodnocovat účinnost preventivních a reaktivních opatření aplikovaných proti KBI,
- navrhovat úpravy bezpečnostní dokumentace společné pro všechny IS KII/VIS na základě zjištění z auditů kybernetické bezpečnosti, z výsledků vyhodnocení účinnosti

systému řízení bezpečnosti informací, a v souvislosti s prováděnými nebo plánovanými změnami v IS KII/VIS,

- zajišťovat testování zálohování a obnovy IS KII/VIS,
- na základě provedení analýzy rizik a hodnocení aktiv provádět aktualizaci dokumentu *Zpráva o hodnocení aktiv a rizik a Plán zvládání rizik*,
- zpracovávat, ve spolupráci s architektem kybernetické bezpečnosti IS KII/VIS a garantem aktiv IS KII/VIS, dokument *Prohlášení o aplikovatelnosti*,
- připravovat podklady do dokumentu *Zpráva z přezkoumání systému řízení bezpečnosti informací* a předkládat je manažerovi kybernetické bezpečnosti,
- garantovat implementaci schválených bezpečnostních opatření,
- do měsíce od informování manažerem kybernetické bezpečnosti ČÚZK zohledňovat reaktivní a ochranná opatření vydaná NBÚ v dokumentu *Zpráva o hodnocení aktiv a rizik*,
- doplnit dokument *Plán zvládání rizik* v případě, že hodnocení rizik aktualizované o nové zranitelnosti spojené s realizací reaktivního nebo ochranného opatření překročí stanovená kritéria pro přijatelnost rizik, a splnění této povinnosti oznámit manažerovi kybernetické bezpečnosti,
- spolupracovat při stanovování provozních pravidel a postupů k zajištění bezpečného provozu IS KII/VIS a navrhovat úpravy dokumentu *Politika řízení provozu a komunikací*,
- stanovovat bezpečnostní požadavky na změny IS KII/VIS spojené s jeho akvizicí, vývojem a údržbou, a uplatňovat jejich zahrnutí do projektu, jehož součástí je akvizice, vývoj a údržba daného IS KII/VIS,
- zpracovávat na základě bezpečnostních potřeb a výsledků hodnocení rizik dokument *Prohlášení o aplikovatelnosti*,
- zajistit vyhodnocení oznámených kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů detekovaných technickými nástroji,

provádět jejich vyhodnocení a přijímat opatření k minimalizaci dopadů v důsledku jejich působení,

- komunikovat s osobami zastávajícími ostatní bezpečnostní role daného IS KII/VIS za účelem zajištění kybernetické bezpečnosti,
- odpovídat za to, že dodavatel provede bezpečnostní testy zranitelnosti aplikací, pokud je provádění bezpečnostních testů začleněno ve smlouvě s dodavatelem.

Práva manažera kybernetické bezpečnosti IS:

- řídit bezpečnost IS a spolupracovat s architektem kybernetické bezpečnosti IS KII/VIS, garantem aktiv IS KII/VIS a administrátory technických aktiv pro zajištění splnění požadavků ZKB a VKB; k tomu vyžadovat součinnost a plnění úkolů,
- vyžadovat spolupráci a konzultaci s manažerem kybernetické bezpečnosti ČÚZK,
- posuzovat žádosti o výjimku a předkládat ke schválení resortnímu MKB, v případech, kdy nelze pravidla, postupy a opatření, stanovená v bezpečnostních dokumentech nebo vyžadovaná ZoKB a VoKB, u IS naplnit.

## 3. Práva a povinnosti architekta kybernetické bezpečnosti IS

Architekt kybernetické bezpečnosti IS zajišťuje návrh bezpečnostních opatření. Odpovídá za návrh bezpečné architektury IS a dohlíží na jeho následnou implementaci.

Povinnosti architekta kybernetické bezpečnosti jsou:

- znalost ZoKB, jeho prováděcích vyhlášek a souvisejících předpisů,
- definovat bezpečnostní požadavky na návrh, vývoj, testování a implementaci IS KII/VIS a změnu stávajících bezpečnostních požadavků,
- zajišťovat bezpečnostní architekturu s cílem zajištění bezpečnosti primárních aktiv, tj. jejich důvěrnosti, dostupnosti a integrity, a to konkrétně:
- posuzovat zajištění bezpečnosti prvků, které tvoří podpůrná aktiva ve vazbě na primární aktiva;
- určovat klíčové podmínky, principy a modely architektury IS KII/VIS, posuzovat a vybírat technologie a stanovovat koncepci bezpečnostního rozvoje IS KII/VIS;
- řídit, koncepčně vést a schvalovat bezpečnostní architekturu informačních a komunikačních systémů včetně podpůrných technických aktiv;
- definovat požadavky na nástroje pro zajištění technických opatření kybernetické bezpečnosti;
- vytvářet a udržovat model architektury kybernetické bezpečnosti (procesní model, aplikační architekturu, technologie atd.);
- navrhovat změny architektury kybernetické bezpečnosti;
- analyzovat úroveň architektury kybernetické bezpečnosti.
- předkládat návrh implementace bezpečnostních opatření,
- vytvářet testovací postupy a odpovídající kritéria akceptace,
- navrhovat a optimalizovat opatření a procesy řešení bezpečnostních událostí a incidentů,
- spolupracovat a předkládat návrhy změn bezpečnostní politiky a bezpečnostních dokumentů,

- dohlížet na implementaci bezpečnostních opatření,
- ve spolupráci s manažerem IS KII/VIS navrhovat opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu,
- provádět kontroly, hodnocení a testování funkčnosti zavedených bezpečnostních opatření,
- poskytovat součinnost dalším bezpečnostním rolím,
- spolupracovat na zajištění trvalé ochrany aplikací a informací IS KII/VIS dostupných z vnější sítě,
- spolupracovat při aplikaci používání kryptografických prostředků a systému správy klíčů.

Právem architekta kybernetické bezpečnosti IS KII/VIS je:

- vyžadovat součinnost příslušného garanta aktiv IS KII/VIS a manažera kybernetické bezpečnosti IS KII/VIS.