

Příloha RD03 - Práva a povinnosti manažera a architekta kybernetické bezpečnosti VIS ISKN

č. sml. Objednatele: ČÚZK- 41763/2022  č. sml. Zhotovitele: CZBAP-1746

# Úvod

Práva a povinnosti manažera i architekta kybernetické bezpečnosti uvedené v tomto dokumentu se týkají VIS ISKN.

# Práva a povinnosti manažera kybernetické bezpečnosti VIS

Manažer kybernetické bezpečnosti VIS odpovídá za systém řízení bezpečnosti informací pro daný VIS a odpovídá se manažeru kybernetické bezpečnosti Objednatele.

## Povinnosti manažera kybernetické bezpečnosti VIS:

* znalost ZoKB a 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 manažerovi kybernetické bezpečnosti Objednatele kybernetické bezpečnostní incidenty VIS a vést jejich evidenci,
* připravovat pro manažera kybernetické bezpečnosti Objednatele podklady pro NÚKIB,
* za VIS připravovat pro manažera kybernetické bezpečnosti Objednatele podklady pro jednání Výboru pro řízení kybernetické bezpečnosti,
* odpovídat za zajištění 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,
* klasifikovat, prošetřovat a určovat příčiny kybernetického bezpečnostního incidentu, vyhodnocovat účinnost preventivních a reaktivních opatření aplikovaných proti kybernetickému bezpečnostnímu incidentu,
* dokumentovat zvládání kybernetických bezpečnostních incidentů,
* navrhovat úpravy bezpečnostní dokumentace na základě zjištění z auditů kybernetické bezpečnosti, výsledků vyhodnocení účinnosti systému řízení bezpečnosti informací a v souvislosti s prováděnými nebo plánovanými změnami ve VIS,
* vyhodnocovat účinnost preventivních a reaktivních opatření aplikovaných proti KBI,
* zajišťovat provedení analýzy rizik a hodnocení aktiv,
* zajišťovat testování zálohování a obnovy IS KII/VIS,
* provádět aktualizaci dokumentu *„Zpráva o hodnocení aktiv a rizik“*, „*Plán zvládání rizik“*, a to nejméně jednou za 3 roky, nebo v souvislosti s prováděnými nebo plánovanými významnými změnami,
* zpracovávat ve spolupráci s architektem kybernetické bezpečnosti VIS a garantem aktiv VIS dokument *„Prohlášení o aplikovatelnosti“*,
* připravovat podklady do dokumentu *„Zpráva z přezkoumání systému řízení bezpečnosti informací“* a předkládat je manažerovi kybernetické bezpečnosti Objednatele,
* garantovat implementaci schválených bezpečnostních opatření,
* zohledňovat, do měsíce od informování manažerem kybernetické bezpečnosti Objednatele, reaktivní a ochranná opatření vydaná NBÚ (nyní NÚKIB) v dokumentu *„Zpráva o hodnocení aktiv a rizik“* a v případě, že hodnocení rizik aktualizované o nové zranitelnosti spojené s realizací reaktivního nebo ochranného opatření překročí stanovená kritéria pro přijatelnost rizik, doplní dokument *„Plán zvládání rizik“*. Splnění oznámí manažerovi kybernetické bezpečnosti,
* stanovovat provozní pravidla a postupy, k zajištění bezpečného provozu VIS, v dokumentu *„Politika řízení provozu a komunikací“*,
* odpovídat za kontrolu přidělování jednoznačného identifikátoru uživatelům VIS,
* odpovídat za to, že Zhotovitel provede bezpečnostní testy zranitelnosti aplikací,
* stanovovat bezpečnostní požadavky na změny VIS spojené s jeho akvizicí, vývojem a údržbou a uplatňovat jejich zahrnutí do projektu, jehož součástí je akvizice, vývoj a údržba daného 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 ostatními bezpečnostními rolemi daného VIS za účelem zajištění kybernetické bezpečnosti,

## Práva manažera kybernetické bezpečnosti VIS:

* řídit a spolupracovat s architektem kybernetické bezpečnosti VIS, garantem aktiv VIS a administrátory technických aktiv pro zajištění splnění požadavků ZoKB a VoKB, k tomu vyžadovat součinnost a plnění úkolů,
* vyžadovat spolupráci a konzultaci s manažerem kybernetické bezpečnosti Objednatele,
* v případech, kdy nelze pravidla, postupy a opatření stanovená v bezpečnostních dokumentech nebo uvedená v ZoKB a VoKB naplnit nebo VIS neumožňuje jejich aplikaci, předkládat opodstatněnou žádost o výjimku, prostřednictvím manažera kybernetické bezpečnosti Objednatele, ke schválení Výboru pro řízení kybernetické bezpečnosti.

# Práva a povinnosti architekta kybernetické bezpečnosti VIS

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

## Povinnosti architekta kybernetické bezpečnosti VIS:

* znalost ZKB, 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.

## Práva architekta kybernetické bezpečnosti VIS:

* vyžadovat součinnost garanta aktiv VIS a manažera kybernetické bezpečnosti VIS.