Národní centrum
kybernetické
bezpečnosti

POMŮCKA K AUDITU BEZPEČNOSTNÍCH OPATŘENÍ PODLE ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI

Verze 2.1

Obsah

1. Úvod

Cílem tohoto dokumentu, je poskytnout rámec bezpečnostních opatření, která jsou pro jednotlivé typy subjektů (správce KII, správce VIS) vyžadována v souladu se zákonem o kybernetické bezpečnosti (zákon č. 181/2014 Sb.) a jeho prováděcího právního předpisu – vyhlášky č. 316/2014 Sb.

Upozornění:

Tento dokument slouží pouze jako podpůrné vodítko při provádění interního auditu bezpečnostních opatření podle zákona o kybernetické bezpečnosti (ZKB), definovaných vyhláškou č. 316/2014 Sb. Dokument nenahrazuje žádný ze zákonů ani souvisejících prováděcích předpisů. Právo změny tohoto dokumentu vyhrazeno.

Tab. 1: Legenda zkratek kontrolních sloupců

Označení	Význam
N	nezavedeno
P	v procesu zavádění
Z	zavedeno
NA	neaplikovatelné

Tab. 2: Vysvětlení sloupců KII a VIS

Vysvětlení	KII	VIS
Uvedená opatření jsou povinni implementovat správci informačních nebo komunikačních systémů KII, správci VIS	X	X
Uvedená opatření jsou povinni implementovat správci informačních nebo komunikačních systémů KII	X	
Uvedená opatření jsou povinni implementovat správci VIS		X

2. Vymezení pojmů

Odkaz	Pojem	Vymezení pojmu
-	Orgán a osoba	Orgán a osoba, které je uložena povinnost v oblasti kybernetické bezpečnosti podle § 3, písmene c) až e) zákona č. 181/2014 Sb. (zákon o kybernetické bezpečnosti).
VKB § 2 a)	Systém řízení bezpečnosti informací (ISMS)	Část systému řízení orgánu a osoby, založená na přístupu k rizikům informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému, která stanoví způsob ustavení, zavádění, provoz, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací.
VKB § 2 b)	Aktivum	Primární a podpůrné aktivum.
VKB § 2 c)	Primární aktivum	Informace nebo služba, kterou zpracovává nebo poskytuje informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém.
VKB § 2 d)	Podpůrné aktivum	Technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.
VKB § 2 e)	Technické aktivum	Technické vybavení, komunikační prostředky a programové vybavení informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému a objekty, ve kterých jsou tyto systémy umístěny.
VKB § 2 f)	Riziko	Možnost, že určitá hrozba využije zranitelnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému a způsobí poškození aktiva.
VKB § 2 g)	Hodnocení rizik	Proces, při němž je určována významnost rizik a jejich přijatelná úroveň.
VKB § 2 h)	Řízení rizik	Činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik.
VKB § 2 i)	Hrozba	Potencionální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, jejímž výsledkem může být poškození aktiva.
VKB § 2 j)	Zranitelnost	Slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami.
VKB § 2 k)	Přijatelné riziko	Riziko zbývající po uplatnění bezpečnostních opatření, jehož úroveň odpovídá kritériím pro přijatelnost rizik. Řízení rizik (VKB § 4)
VKB § 2 l)	Bezpečnostní politika	Soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv orgánem a osobou.
VKB § 2 m)	Garant aktiva	Fyzická osoba pověřená orgánem a osobou k zajištění rozvoje, použití a bezpečnosti aktiva.
VKB § 2 n)	Uživatel	Fyzická nebo právnická osoba anebo orgán veřejné moci, která využívá primární aktiva.
VKB § 2 o)	Administrátor	Fyzická osoba pověřená garantem aktiva odpovědná za správu, provoz, použití, údržbu a bezpečnost technického aktiva.
VKB § 6 odst. 4	Manažer kybernetické bezpečnosti	Osoba odpovědná za systém řízení bezpečnosti informací, která je pro tuto činnost řádně vyškolena a prokáže odbornou způsobilost praxí s řízením bezpečnosti informací po dobu nejméně tří let.
VKB § 6	Architekt kybernetické bezpečnosti	Osoba odpovědná za návrh a implementaci bezpečnostních opatření, která je pro tuto činnost řádně vyškolena a

odst. 5		prokáže odbornou způsobilost praxí s navrhováním bezpečnostní architektury po dobu nejméně tří let.
VKB § 6 odst. 6	Auditor kybernetické bezpečnosti	Osoba odpovědná za provádění auditu kybernetické bezpečnosti, která je pro tuto činnost řádně vyškolena a prokáže odbornou způsobilost praxí s prováděním auditů kybernetické bezpečnosti po dobu nejméně tří let. Auditor kybernetické bezpečnosti vykonává svoji roli nestranně a výkon jeho role je oddělen od výkonu rolí manažera, architekta a výboru kybernetické bezpečnosti.
VKB § 6 odst. 7	Výbor pro řízení kybernetické bezpečnosti	Organizovaná skupina tvořená osobami, které jsou pověřeny celkovým řízením a rozvojem informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému, anebo se významně podílejí na řízení a koordinaci činností spojených s kybernetickou bezpečností těchto systémů.
VKB § 16 odst. 3	Prostředky fyzické bezpečnosti	Prostředky fyzické bezpečnosti jsou zejména: a) mechanické zábranné prostředky, b) zařízení elektrické zabezpečovací signalizace, c) prostředky omezující působení požárů, d) prostředky omezující působení projevů živelních událostí, e) systémy pro kontrolu vstupu, f) kamerové systémy, g) zařízení pro zajištění ochrany před selháním dodávky elektrického napájení a h) zařízení pro zajištění optimálních provozních podmínek.
VKB § 18 odst. 2	Nástroj pro ověřování identity uživatelů a administrátorů	Nástroj pro ověřování identity uživatelů a administrátorů zajišťuje ověření identity uživatelů a administrátorů před zahájením jejich aktivit v informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury a významném informačním systému.

3. Bezpečnostní opatření

3.1. Organizační opatření

3.1.1. Systém řízení bezpečnosti informací (VKB § 3)

(souhrnný charakter)

KII	VIS			N	P	Z	NA
X		odst. 1 a)	Je stanoven rozsah ISMS.				
X	X	odst. 1 b) odst. 2 a)	Je zaveden proces řízení rizik.				
X	X	odst. 1 c) odst. 2 b)	Jsou vytvořeny, schváleny a zavedeny bezpečnostní politiky v oblasti ISMS, zavedena příslušná bezpečnostní opatření.				
X		odst. 1 d)	Zaveden proces monitorování účinnosti bezpečnostních opatření.				
X		odst. 1 e)	Zaveden proces vyhodnocování vhodnosti a účinnosti bezpečnostní politiky.				
X		odst. 1 f)	Audit kybernetické bezpečnosti je prováděn nejméně 1-krát ročně.				
X		odst. 1 g)	Zajištěno vyhodnocení účinnosti ISMS, které obsahuje hodnocení stavu ISMS včetně revize hodnocení rizik, posouzeny výsledky provedených kontrol a auditů kybernetické bezpečnosti a dopadů kybernetických bezpečnostních incidentů na systém řízení bezpečnosti informací, a to nejméně 1-krát ročně.				
X		odst. 1 h)	Je prováděna aktualizace ISMS a související dokumentace na základě zjištění auditů kybernetické bezpečnosti, výsledků hodnocení účinnosti ISMS a v souvislosti s prováděnými změnami.				
X		odst. 1 i)	Řízen provoz a zdroje ISMS, zaznamenávány činnosti spojené s ISMS a souvisejícím řízením rizik.				
	X	odst. 2 c)	Prováděna aktualizace zprávy o hodnocení aktiv a rizik, bezpečnostní politiky, plánu zvládání rizik a plánu rozvoje bezpečnostního povědomí, a to nejméně jednou za tři roky nebo v souvislosti s prováděnými nebo plánovanými změnami.				

3.1.2. Řízení rizik (VKB § 4)

KII	VIS			N	P	Z	NA
X	X	odst. 1, 2 a)	Stanoveny metodiky pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik včetně stanovení kritérií pro přijatelnost rizik.				
X	X	odst. 1, 2 b)	Prováděna identifikace a hodnocení důležitosti aktiv, která patří do rozsahu ISMS, podle § 8 (Řízení aktiv) minimálně v rozsahu přílohy č. 1 k VKB a výstupy zapracuje do zprávy o hodnocení aktiv a rizik.				
X	X	odst. 1, 2 c)	Prováděna identifikace rizik, při kterých jsou zohledňovány hrozby a zranitelnosti, posuzovány možné dopady na aktiva, hodnotí tato rizika minimálně v rozsahu podle přílohy č. 2 k VKB. Jsou určena a schválena přijatelná rizika a je zpracována zpráva o hodnocení aktiv a rizik.				
X	X	odst. 1, 2 d)	Na základě bezpečnostních potřeb a výsledků hodnocení rizik je zpracováváno prohlášení o aplikovatelnosti, které obsahuje přehled vybraných a zavedených bezpečnostních opatření.				
X	X	odst. 1, 2 e)	Je zpracovaný a zavedený plán zvládání rizik, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání rizik, určení osoby odpovědné za prosazování bezpečnostních opatření pro zvládání rizik, potřebné finanční, technické, lidské a informační zdroje, termín jejich zavedení a popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními.				
X	X	odst. 1, 2 f)	Bez zbytečného odkladu jsou zohledňována reaktivní a ochranná opatření vydaná NBÚ v hodnocení rizik a v případě, že hodnocení rizik aktualizované o nové zranitelnosti spojené s realizací reaktivního nebo ochranného opatření překročí stanovená kritéria pro přijatelnost rizik, jsou doplněny plány zvládání rizik.				
X	X	odst. 3	Řízení rizik je zajištěno jinými způsoby (než jak je stanoveno v odstavci 1 a 2) a orgán a osoba doložil(a), že použitá opatření zajišťují stejnou nebo vyšší úroveň řízení rizik.				
		Zváženy hrozby, související s/se:					
X	X	odst. 4 a)	porušením bezpečnostní politiky, provedením neoprávněných činností, zneužitím oprávnění ze strany uživatelů a administrátorů.				
X	X	odst. 4 b)	poškozením nebo selháním technického anebo programového vybavení.				
X	X	odst. 4 c)	zneužití identity fyzické osoby.				
X	X	odst. 4 d)	užíváním programového vybavení v rozporu s licenčními podmínkami.				
X	X	odst. 4 e)	kybernetickým útokem z komunikační sítě.				
X	X	odst. 4 f)	škodlivým kódem (například viry, spyware, trojské koně).				
X	X	odst. 4 g)	nedostatky při poskytování služeb informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.				
X	X	odst. 4 h)	narušením fyzické bezpečnosti.				
X	X	odst. 4 i)	přerušením poskytování služeb elektronických komunikací nebo dodávek elektrické energie.				
X	X	odst. 4 j)	zneužitím nebo neoprávněnou modifikací údajů.				
X	X	odst. 4 k)	trvale působícími hrozbami.				
X	X	odst. 4 l)	odcizením nebo poškozením aktiva.				
X		odst. 6 a)	Porušením bezpečnostní politiky, provedením neoprávněných činností, zneužitím oprávnění ze strany administrátorů kritické informační infrastruktury.				

X		odst. 6 b)	Pochybením ze strany zaměstnanců.				
X		odst. 6 c)	Zneužitím vnitřních prostředků, sabotáží.				
X		odst. 6 d)	Dlouhodobým přerušením poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb.				
X		odst. 6 e)	Nedostatkem zaměstnanců s potřebnou odbornou úrovní.				
X		odst. 6 f)	Cíleným kybernetickým útokem pomocí sociálního inženýrství, použitím špionážních technik.				
X		odst. 6 g)	Zneužitím vyměnitelných technických nosičů dat.				
		Zváženy zranitelnosti, související s:					
X	X	odst. 5 a)	nedostatečnou ochranou vnějšího perimetru.				
X	X	odst. 5 b)	nedostatečným bezpečnostním povědomím uživatelů a administrátorů.				
X	X	odst. 5 c)	nedostatečnou údržbou informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.				
X	X	odst. 5 d)	nevhodným nastavením přístupových oprávnění.				
X	X	odst. 5 e)	nedostatečnými postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů.				
X	X	odst. 5 f)	nedostatečným monitorováním činností uživatelů a administrátorů a neschopností odhalit jejich nevhodné nebo závadné způsoby chování.				
X	X	odst. 5 g)	nedostatečným stanovením bezpečnostních pravidel, nepřesným nebo nejednoznačným vymezením práv a povinností uživatelů, administrátorů a bezpečnostních rolí.				
X		odst. 7 a)	Nedostatečnou ochranou prostředků kritické informační infrastruktury.				
X		odst. 7 b)	Nevhodnou bezpečnostní architekturou.				
X		odst. 7 c)	Nedostatečnou mírou nezávislé kontroly.				
X		odst. 7 d)	Neschopností včasného odhalení pochybení ze strany zaměstnanců.				

3.1.3. Bezpečnostní politika (VKB § 5)

KII	VIS			N	P	Z	NA
		Stanovena bezpečnostní politika v oblastech:					
X	X	odst. 1 a) odst. 2 a)	Systém řízení bezpečnosti informací.				
X	X	odst. 1 b) odst. 2 b)	Organizační bezpečnost. (*Organizační bezpečnost (VKB § 6)*)				
X		odst. 1 c)	Řízení vztahů s dodavateli. (*Stanovení bezpečnostních požadavků pro dodavatele (VKB § 7)*)				
	X	odst. 2 c)	Řízení dodavatelů. (*Stanovení bezpečnostních požadavků pro dodavatele (VKB § 7)*)				
X	X	odst. 1 d) odst. 2 d)	Klasifikace aktiv.				
X	X	odst. 1 e) odst. 2 e)	Bezpečnost lidských zdrojů.				
X	X	odst. 1 f) odst. 2 f)	Řízení provozu a komunikací.				
X	X	odst. 1 g) odst. 2 g)	Řízení přístupu.				
X	X	odst. 1 h) odst. 2 h)	Bezpečné chování uživatelů.				
X	X	odst. 1 i) odst. 2 i)	Zálohování a obnova.				
X		odst. 1 j)	Bezpečné předávání a výměna informací.				
X		odst. 1 k)	Řízení technických zranitelností.				
X		odst. 1 l)	Bezpečné používání mobilních zařízení.				
X	X	odst. 1 m) odst. 2 j)	Poskytování a nabývání licencí programového vybavení a informací.				
X		odst. 1 n)	Dlouhodobé ukládání a archivace informací.				
X	X	odst. 1 o) odst. 2 k)	Ochrana osobních údajů.				
X		odst. 1 p)	Fyzická bezpečnost.				
X		odst. 1 q)	Bezpečnost komunikační sítě.				
X	X	odst. 1 r) odst. 2 m)	Ochrana před škodlivým kódem.				
X	X	odst. 1 s) odst. 2 n)	Nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí.				
X		odst. 1 t)	Využití a údržba nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí.				

X	X	odst. 1 u) odst. 2 l)	Používání kryptografické ochrany.				
X	X	odst. 3	Je pravidelně hodnocena účinnost bezpečnostní politiky. Bezpečnostní politika je pravidelně aktualizována.				

3.1.4. Organizační bezpečnost (VKB § 6)

KII	VIS			N	P	Z	NA
X	X	odst. 1	Zavedena organizace řízení bezpečnosti informací (dále jen „organizační bezpečnost“), v rámci které je určen výbor pro řízení kybernetické bezpečnosti a bezpečnostní role a jejich práva a povinnosti související s informačním systémem kritické informační infrastruktury, komunikačním systémem kritické informační infrastruktury nebo významným informačním systémem.				
X		odst. 2 a)	Určena bezpečnostní role: manažer kybernetické bezpečnosti.				
X		odst. 2 b)	Určena bezpečnostní role: architekt kybernetické bezpečnosti.				
X		odst. 2 c)	Určena bezpečnostní role: auditor kybernetické bezpečnosti.				
X		odst. 2 d)	Určena bezpečnostní role: garant aktiva (podle § 2 písmene m).				
	X	odst. 3	Bezpečnostní role jsou určeny přiměřeně podle odstavce 2.				
X	X	odst. 7	Určen výbor pro řízení kybernetické bezpečnosti.				
X	X	odst. 8	Je zajištěno odborné školení osob, které zastávají bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí podle *Bezpečnost lidských* zdrojů odst. 1 písm. b).				

3.1.5. Stanovení bezpečnostních požadavků pro dodavatele (VKB § 7)

KII	VIS			N	P	Z	NA
X	X	odst. 1	Jsou stanovena pravidla pro dodavatele, která zohledňují potřeby řízení bezpečnosti informací, a řídí své dodavatele nebo jiné externí subjekty, které se podílejí na rozvoji, provozu nebo zajištění bezpečnosti IS nebo KS KII a VIS. Rozsah zapojení dodavatelů na rozvoji, provozu nebo zajištění bezpečnosti IS nebo KS KII a VIS dokumentován písemnou smlouvou, jejíž součástí je ustanovení o bezpečnosti informací.				
X		odst. 2 a)	U dodavatelů uvedených v odstavci 1 je před uzavřením smlouvy prováděno hodnocení rizik (podle přílohy č. 2 k VKB), která jsou spojena s podstatnými dodávkami.				
X		odst. 2 b)	U dodavatelů uvedených v odstavci 1 uzavírá smlouvu o úrovni služeb, která stanoví způsoby a úrovně realizace bezpečnostních opatření a určí vztah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření.				
X		odst. 2 c)	U dodavatelů uvedených v odstavci 1 provádí pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných služeb a zjištěné nedostatky odstraňuje nebo po dohodě s dodavatelem zajistí jejich odstranění.				

3.1.6. Řízení aktiv (VKB § 8)

KII	VIS			N	P	Z	NA
X	X	odst. 1 a)	Jsou identifikována a evidována primární aktiva.				
X	X	odst. 1 b)	Jsou určeni jednotliví garanti aktiv, kteří jsou odpovědní za primární aktiva.				
X	X	odst. 1 c)	Je hodnocena důležitost primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti a tato aktiva jsou zařazena do jednotlivých úrovní minimálně v rozsahu podle přílohy č. 1 k VKB.				
		Při hodnocení důležitosti primárních aktiv je posouzeno především:					
X	X	odst. 2 a)	Rozsah a důležitost osobních údajů nebo obchodního tajemství.				
X	X	odst. 2 b)	Rozsah dotčených právních povinností nebo jiných závazků.				
X	X	odst. 2 c)	Rozsah narušení vnitřních řídících a kontrolních činností.				
X	X	odst. 2 d)	Poškození veřejných, obchodních nebo ekonomických zájmů.				
X	X	odst. 2 e)	Možné finanční ztráty.				
X	X	odst. 2 f)	Rozsah narušení běžných činností orgánu a osoby.				
X	X	odst. 2 g)	Dopady spojené s narušením důvěrnosti, integrity a dostupnosti.				
X	X	odst. 2 h)	Dopady na zachování dobrého jména nebo ochranu dobré pověsti.				
X		odst. 3 a)	Jsou identifikována a evidována podpůrná aktiva.				
X		odst. 3 b)	Jsou určeni garanti aktiv, kteří jsou odpovědní za podpůrná aktiva.				
X		odst. 3 c)	Jsou určeny vazby mezi primárními a podpůrnými aktivy a hodnoceny důsledky závislostí mezi primárními a podpůrnými aktivy.				
		Jsou stanovena pravidla ochrany, nutná pro zabezpečení jednotlivých úrovní aktiv tím, že:					
X	X	odst. 4 a) 1.	Jsou určeny způsoby rozlišování jednotlivých úrovní aktiv.				
X	X	odst. 4 a) 2.	Jsou stanovena pravidla pro manipulaci a evidenci s aktivy podle úrovní aktiv, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv.				
X	X	odst. 4 a) 3.	Jsou stanoveny přípustné způsoby používání aktiv.				
X	X	odst. 4 b)	Jsou zavedena pravidla ochrany odpovídající úrovni aktiv.				
X	X	odst. 4 c)	Jsou určeny způsoby pro spolehlivé smazání nebo ničení technických nosičů dat s ohledem na úroveň aktiv.				

3.1.7. Bezpečnost lidských zdrojů (VKB § 9)

KII	VIS			N	P	Z	NA
X	X	odst. 1 a)	Je stanoven plán rozvoje bezpečnostního povědomí, který obsahuje formu, obsah a rozsah potřebných školení a jsou určeny osoby provádějící realizaci jednotlivých činností, které jsou v plánu uvedeny.				
X	X	odst. 1 b)	V souladu s plánem rozvoje bezpečnostního povědomí je zajištěno poučení uživatelů, administrátorů a osob zastávajících bezpečnostní role o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení.				
X	X	odst. 1 c)	Je zajištěna kontrola dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.				
X	X	odst. 1 d)	Je zajištěno vrácení svěřených aktiv a odebrání přístupových oprávnění při ukončení smluvního vztahu s uživateli, administrátory nebo osobami zastávajícími bezpečnostní role.				
X	X	odst. 2	O školení podle odstavce 1 jsou vedeny přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.				
X		odst. 3 a)	Jsou stanovena pravidla pro určení osob, které budou zastávat bezpečnostní role, role administrátorů nebo uživatelů.				
X		odst. 3 b)	Je hodnocena účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených s prohlubováním bezpečnostního povědomí.				
X		odst. 3 c)	Jsou určena pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.				
X		odst. 3 d)	Zajištěna změna přístupových oprávnění při změně postavení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role.				

3.1.8. Řízení provozu a komunikací (VKB § 10)

KII	VIS			N	P	Z	NA
X	X	odst. 1	Pomocí technických nástrojů uvedených v § 21 až 23 jsou detekovány kybernetické bezpečnostní události, pravidelně vyhodnocovány získané informace a na zjištěné nedostatky reagováno v souladu s: *Zvládání kybernetických bezpečnostních událostí a incidentů (VKB § 13)*.				
X	X	odst. 2	Zajištěn bezpečný provoz informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému. Za tímto účelem jsou stanoveny provozní pravidla a postupy.				
X	X	odst. 4	Je prováděno pravidelné zálohování a prověřování použitelnosti provedených záloh.				
		Provozní pravidla a postupy orgánu a osoby obsahují:					
X		odst. 3 a)	Práva a povinnosti osob zastávajících bezpečnostní role, administrátorů a uživatelů.				
X		odst. 3 b)	Postupy pro spuštění a ukončení chodu systému, pro restart nebo obnovení chodu systému po selhání a pro ošetření chybových stavů nebo mimořádných jevů.				
X		odst. 3 c)	Postupy pro sledování kybernetických bezpečnostních událostí a pro ochranu přístupu k záznamům o těchto činnostech.				
X		odst. 3 d)	Spojení na kontaktní osoby, které jsou určeny jako podpora při řešení neočekávaných systémových nebo technických potíží.				
X		odst. 3 e)	Postupy řízení a schvalování provozních změn.				
X		odst. 3 f)	Postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů.				
X		odst. 5 a)	Je zajištěno oddělení vývojového, testovacího a produkčního prostředí.				
X		Jsou řešena reaktivní opatření vydaná NBÚ tím, že orgán a osoba:					
X		odst. 5 b) 1.	Posuzuje očekávané dopady reaktivního opatření na informační systém kritické informační infrastruktury nebo komunikační systém kritické informační infrastruktury a na zavedená bezpečnostní opatření, vyhodnocuje možné negativní účinky a bez zbytečného odkladu je oznamuje NBÚ.				
X		odst. 5 b) 2.	Stanovuje způsob rychlého provedení reaktivního opatření, který minimalizuje možné negativní účinky, a určuje časový plán jeho provedení.				
X		odst. 6 a)	Je zajištěna bezpečnost a integrita komunikačních sítí a bezpečnost komunikačních služeb podle *Nástroj pro ochranu integrity komunikačních sítí (VKB § 17)*.				
X		odst. 6 b)	Jsou určeny pravidla a postupy pro ochranu informací, které jsou přenášeny komunikačními sítěmi.				
X		odst. 6 c)	Výměna a předávání informací je prováděna na základě pravidel stanovených právními předpisy za současného zajištění bezpečnosti informací a tato pravidla jsou dokumentována.				
X		odst. 6 d)	S ohledem na klasifikaci aktiv je prováděna výměna a předávání informací na základě písemných smluv, jejichž součástí je ustanovení o bezpečnosti informací.				

3.1.9. Řízení přístupu a bezpečné chování uživatelů (VKB § 11)

KII	VIS			N	P	Z	NA
X	X	odst. 1	Na základě provozních a bezpečnostních potřeb je řízen přístup k informačnímu systému kritické informační infrastruktury, komunikačnímu systému kritické informační infrastruktury a významnému informačnímu systému a každému uživateli je přiřazen jednoznačný identifikátor.				
X	X	odst. 2	Jsou přijata opatření, která slouží k zajištění ochrany údajů, které jsou používány pro přihlášení uživatelů a administrátorů informačního systému kritické informační struktury, komunikačního systému kritické informační infrastruktury a významného informačního systému podle *Nástroj* pro ověřování identity uživatelů (VKB § 18) a *Nástroj pro řízení přístupových oprávnění (VKB § 19)*, a která brání ve zneužití těchto údajů neoprávněnou osobou.				
X		odst. 3 a)	Přistupujícím aplikacím je přidělen samostatný identifikátor.				
X		odst. 3 b)	Je omezeno přidělování administrátorských oprávnění.				
X		odst. 3 c)	Přidělování a odebírání přístupových oprávnění je prováděno v souladu s politikou řízení přístupu.				
X		odst. 3 d)	Je prováděno pravidelné přezkoumání nastavení přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách nebo rolích.				
X		odst. 3 e)	Je využíván nástroj pro ověřování identity uživatelů podle *Nástroj* pro ověřování identity uživatelů (VKB § 18) a nástroj pro řízení přístupových oprávnění podle *Nástroj pro řízení přístupových oprávnění (VKB § 19)*.				
X		odst. 3 f)	Jsou zavedena bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení, případně i bezpečnostní opatření spojená s využitím technických zařízení, kterými povinná osoba nedisponuje.				

3.1.10. Akvizice, vývoj a údržba (VKB § 12)

KII	VIS			N	P	Z	NA
X	X	odst. 1	Jsou stanoveny bezpečnostní požadavky na změny informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému spojené s jejich akvizicí, vývojem a údržbou a jsou zahrnuty do projektu akvizice, vývoje a údržby systému.				
X		odst. 2 a)	Jsou identifikována, hodnocena a řízena rizika související s akvizicí, vývojem a údržbou informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury; pro postupy hodnocení a řízení rizik se metodiky podle *Řízení rizik* (VKB § 4) odst. 1 písm. a) použijí obdobně.				
X		odst. 2 b)	Je zajištěna bezpečnost vývojového prostředí a zároveň je zajištěna ochrana používaných testovacích dat.				
X		odst. 2 c)	Je prováděno bezpečnostní testování změn informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury před jejich zavedením do provozu.				

3.1.11. Zvládání kybernetických bezpečnostních událostí a incidentů (VKB § 13)

KII	VIS			N	P	Z	NA
X	X	a)	Jsou přijata nezbytná opatření, která zajistí oznamování kybernetických bezpečnostních událostí u informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a o oznámeních jsou vedeny záznamy.				
X	X	b)	Je připraveno prostředí pro vyhodnocení oznámených kybernetických bezpečnostních událostí a kybernetických bezpečnostních událostí detekovaných technickými nástroji podle *Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů (VKB § 21)*, *Nástroj pro detekci kybernetických bezpečnostních událostí (VKB §* 22), *Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí (VKB § 23)*, je prováděno jejich vyhodnocení a jsou identifikovány kybernetické bezpečnostní incidenty.				
X	X	c)	Je prováděna klasifikace kybernetických bezpečnostních incidentů, přijímáno opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu, prováděno hlášení kybernetického bezpečnostního incidentu podle § 32 a zajištěn sběr věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu.				
X	X	d)	Jsou prošetřeny a určeny příčiny kybernetického bezpečnostního incidentu, vyhodnocena účinnost řešení kybernetického bezpečnostního incidentu a na základě vyhodnocení jsou stanovena nutná bezpečnostní opatření k zamezení opakování řešeného kybernetického bezpečnostního incidentu.				
X	X	e)	Zvládání kybernetických bezpečnostních incidentů je dokumentováno.				

3.1.12. Řízení kontinuity činností (VKB § 14)

KII	VIS			N	P	Z	NA
X	X	odst. 1 a)	Jsou stanoveny práva a povinnosti garantů aktiv, administrátorů a osob zastávajících bezpečnostní role.				
		Jsou stanoveny cíle řízení kontinuity činností formou určení:					
X	X	odst. 1 b) 1.	Minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.				
X	X	odst. 1 b) 2.	Doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.				
X	X	odst. 1 b) 3.	Doby obnovení dat jako termínu, ke kterému budou obnovena data po kybernetickém bezpečnostním incidentu.				
X	X	odst. 1 c)	Je stanovena strategie řízení kontinuity činností, která obsahuje naplnění cílů podle písmene b).				
X		odst. 2 a)	Jsou vyhodnocovány a dokumentovány možné dopady kybernetických bezpečnostních incidentů a posouzena možná rizika související s ohrožením kontinuity činností.				
X		odst. 2 b)	Jsou stanoveny, aktualizovány a pravidelně testovány plány kontinuity činností informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury.				
X		odst. 2 c)	Jsou realizována opatření pro zvýšení odolnosti informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury vůči kybernetickému bezpečnostnímu incidentu a je využíván nástroj pro zajišťování úrovně dostupnosti podle *Nástroj pro zajišťování úrovně dostupnosti (VKB § 26)*.				
		Jsou stanoveny a aktualizovány postupy pro provedení opatření vydaných NBÚ podle § 13 a 14 ZKB, ve kterých je zohledněno:					
X		odst. 2 d) 1.	Výsledky hodnocení rizik provedení opatření.				
X		odst. 2 d) 2.	Stav dotčených bezpečnostních opatření.				
X		odst. 2 d) 3.	Vyhodnocení případných negativních dopadů na provoz a bezpečnost informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury				

3.1.13. Kontrola a audit kybernetické bezpečnosti (VKB § 15)

KII	VIS			N	P	Z	NA
X	X	odst. 1 a)	Je posouzen soulad bezpečnostních opatření s obecně závaznými právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k informačnímu systému kritické informační infrastruktury, komunikačnímu systému kritické informační infrastruktury a VIS a určena opatření pro jeho prosazování.				
X	X	odst. 1 b)	Jsou prováděny a dokumentovány pravidelné kontroly dodržování bezpečnostní politiky a výsledky těchto kontrol jsou zohledněny v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik.				
X		odst. 2	Je zajištěno provedení auditu kybernetické bezpečnosti osobou s odbornou kvalifikací podle § 6 odst. 6 VKB (auditor kybernetické bezpečnosti), která hodnotí správnost a účinnost zavedených bezpečnostních opatření.				
X		odst. 3	Pro IS nebo KS KII je prováděna kontrola zranitelnosti technických prostředků pomocí automatizovaných nástrojů a jejich odborné vyhodnocování a je reagováno na zjištěné zranitelnosti.				

3.2. Technická opatření

3.2.1. Fyzická bezpečnost (VKB § 16)

KII	VIS			N	P	Z	NA
X	X	odst. 1 a)	Jsou přijata nezbytná opatření k zamezení neoprávněnému vstupu do vymezených prostor, kde jsou zpracovávány informace a umístěna technická aktiva informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.				
X	X	odst. 1 b)	Jsou přijata nezbytná opatření k zamezení poškození a zásahům do vymezených prostor, kde jsou uchovány informace a umístěna technická aktiva informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.				
X	X	odst. 1 c)	Je předcházeno poškození, krádeži nebo kompromitaci aktiv nebo přerušení poskytování služeb informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.				
X		odst. 2 a)	Jsou uplatněny prostředky fyzické bezpečnosti pro zajištění ochrany na úrovni objektů.				
X		odst. 2 b)	Jsou uplatněny prostředky fyzické bezpečnosti pro zajištění ochrany v rámci objektů zajištěním zvýšené bezpečnosti vymezených prostor, ve kterých jsou umístěna technická aktiva informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury.				

3.2.2. Nástroj pro ochranu integrity komunikačních sítí (VKB § 17)

KII	VIS			N	P	Z	NA
		Pro ochranu integrity rozhraní vnější komunikační sítě, která není pod správou orgánu nebo osoby, a vnitřní komunikační sítě, která je pod správou orgánu nebo osoby, je zavedeno(a):					
X	X	odst. 1 a)	Řízení bezpečného přístupu mezi vnější a vnitřní sítí.				
X	X	odst. 1 b)	Segmentace zejména použitím demilitarizovaných zón jako speciálního typu sítě používaného ke zvýšení bezpečnosti aplikací dostupných z vnější sítě a k zamezení přímé komunikace vnitřní sítě s vnější sítí.				
X	X	odst. 1 c)	Použití kryptografických prostředků (*Kryptografické prostředky* (VKB § 25)) pro vzdálený přístup, vzdálenou správu nebo pro přístup pomocí bezdrátových technologií.				
X	X	odst. 1 d)	Opatření pro odstranění nebo blokování přenášených dat, která neodpovídají požadavkům na ochranu integrity komunikační sítě.				
X		odst. 2	Jsou využívány nástroje pro ochranu integrity vnitřní komunikační sítě, které zajistí její segmentaci.				

3.2.3. Nástroj pro ověřování identity uživatelů (VKB § 18)

KII	VIS			N	P	Z	NA
X	X	odst. 1	Jsou používány nástroje pro ověření identity uživatelů a administrátorů informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému.				
		Nástroj pro ověřování identity uživatelů, který používá autentizaci pouze heslem, zajišťuje:					
X	X	odst. 3 a)	Minimální délku hesla osm znaků.				
X	X	odst. 3 b)	Minimální složitost hesla tak, že heslo bude obsahovat alespoň tři z následujících čtyř požadavků: 1. nejméně jedno velké písmeno, 2. nejméně jedno malé písmeno, 3. nejméně jednu číslici nebo 4. nejméně jeden speciální znak, který není uveden v bodech 1 až 3.				
X	X	odst. 3 c)	Maximální dobu pro povinnou výměnu hesla nepřesahující sto dnů; tento požadavek není vyžadován pro samostatné identifikátory aplikací.				
X	X	odst. 5	**Nástroj pro ověřování identity uživatelů je zajištěn jinými způsoby, než jaké jsou stanoveny v odstavcích 3 až 5, a orgán a osoba doložil(a), že použitá opatření zajišťují stejnou nebo vyšší úroveň odolnosti hesla.**				
		Je používán nástroj pro ověřování identity, který:					
X		odst. 4 a) 1.	Zamezuje opětovnému používání dříve používaných hesel a neumožní více změn hesla jednoho uživatele během stanoveného období, které musí být nejméně 24 hodin.				
X		odst. 4 a) 2.	Provádí opětovné ověření identity po určené době nečinnosti.				
X		odst. 4 b)	Využívá nástroj pro ověřování identity administrátorů. V případě, že tento nástroj využívá autentizaci heslem, zajistí prosazení minimální délky hesla patnáct znaků při dodržení požadavků podle odstavce 3 písm. b) a c).				

3.2.4. Nástroj pro řízení přístupových oprávnění (VKB § 19)

KII	VIS			N	P	Z	NA
X	X	Je používán nástroj pro řízení přístupových oprávnění, kterým zajišťuje řízení oprávnění:					
X	X	odst. 1 a)	Pro přístup k jednotlivým aplikacím a datům.				
X	X	odst. 1 b)	Pro čtení dat, pro zápis dat a pro změnu oprávnění.				
X		odst. 2	Je používán nástroj pro řízení přístupových oprávnění, který zaznamenává použití přístupových oprávnění v souladu s bezpečnostními potřebami a výsledky hodnocení rizik.				

3.2.5. Nástroj pro ochranu před škodlivým kódem (VKB § 20)

KII	VIS			N	P	Z	NA
		Pro řízení rizik spojených s působením škodlivého kódu je používán nástroj pro ochranu informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému před škodlivým kódem, který zajistí ověření a stálou kontrolu:					
X	X	odst. 1 a)	Komunikace mezi vnitřní sítí a vnější sítí.				
X	X	odst. 1 b)	Serverů a sdílených datových úložišť.				
X	X	odst. 1 c)	Pracovních stanic.				
X	X		Je prováděna pravidelná aktualizace nástroje pro ochranu před škodlivým kódem, jeho definic a signatur.				

3.2.6. Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů (VKB § 21)

KII	VIS			N	P	Z	NA
X	X	Je používán nástroj pro zaznamenávání činností informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému, který zajišťuje:					
X	X	odst. 1 a)	Sběr informací o provozních a bezpečnostních činnostech, zejména typ činnosti, datum a čas, identifikaci technického aktiva, které činnost zaznamenalo, identifikaci původce a místa činnosti a úspěšnost nebo neúspěšnost činnosti.				
X	X	odst. 1 b)	Ochranu získaných informací před neoprávněným čtením nebo změnou.				
X	X	Pomocí nástroje pro zaznamenávání činnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému je zaznamenáváno(y):					
X	X	odst. 2 a)	Přihlášení a odhlášení uživatelů a administrátorů.				
X	X	odst. 2 b)	Činnosti provedené administrátory.				
X	X	odst. 2 c)	Činnosti vedoucí ke změně přístupových oprávnění.				
X	X	odst. 2 d)	Neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů.				
X	X	odst. 2 e)	Zahájení a ukončení činností technických aktiv informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému.				
X	X	odst. 2 f)	Automatická varovná nebo chybová hlášení technických aktiv.				
X	X	odst. 2 g)	Přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností.				
X	X	odst. 2 h)	Použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.				
X	X	odst. 4	Nejméně jednou za 24 hodin je prováděna synchronizace jednotného systémového času technických aktiv patřících do informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.				
X		odst. 3	Záznamy činností zaznamenané podle odst. 2 jsou uchovávány nejméně po dobu tří měsíců.				

3.2.7. Nástroj pro detekci kybernetických bezpečnostních událostí (VKB § 22)

KII	VIS			N	P	Z	NA
X	X	odst. 1	Je používán nástroj pro detekci kybernetických bezpečnostních událostí, který vychází ze stanovených bezpečnostních potřeb a výsledků hodnocení rizik a který zajistí ověření, kontrolu a případné zablokování komunikace mezi vnitřní komunikační sítí a vnější sítí.				
		Je používán nástroj pro detekci kybernetických bezpečnostních událostí, který zajistí ověření, kontrolu a případně zablokování komunikace:					
X		odst. 2 a)	V rámci vnitřní komunikační sítě.				
X		odst. 2 b)	Serverů patřících do informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury.				

3.2.8. Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí (VKB § 23)

KII	VIS			N	P	Z	NA
		Je používán nástroj pro sběr a průběžné vyhodnocování kybernetických bezpečnostních událostí, který v souladu s bezpečnostními potřebami a výsledky hodnocení rizik zajišťuje:					
X		odst. 1 a)	Integrovaný sběr a vyhodnocení kybernetických bezpečnostních událostí z informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury.				
X		odst. 1 b)	Poskytování informací pro určené bezpečnostní role o detekovaných kybernetických bezpečnostních událostech v informačním systému kritické informační infrastruktury nebo komunikačním systému kritické informační infrastruktury.				
X		odst. 1 c)	Nepřetržité vyhodnocování kybernetických bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů, včetně včasného varování určených bezpečnostních rolí.				
X		odst. 2 a)	Je zajištěna pravidelná aktualizace nastavení pravidel pro vyhodnocování kybernetických bezpečnostních událostí a včasné varování, aby byly omezovány případy nesprávného vyhodnocení událostí nebo případy falešných varování.				
X		odst. 2 b)	Zajištěno využívání informací, které jsou připraveny nástrojem pro sběr a vyhodnocení kybernetických bezpečnostních událostí, pro optimální nastavení bezpečnostních opatření informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury.				

3.2.9. Aplikační bezpečnost (VKB § 24)

KII	VIS			N	P	Z	NA
X	X	odst. 1	Jsou prováděny bezpečnostní testy zranitelnosti aplikací, které jsou přístupné z vnější sítě, a to před jejich uvedením do provozu a po každé zásadní změně bezpečnostních mechanismů.				
X		odst. 2 a)	Je zajištěna trvalá ochrana aplikací a informací dostupných z vnější sítě před neoprávněnou činností, popřením provedených činností, kompromitací nebo neautorizovanou změnou.				
X		odst. 2 b)	Je zajištěna trvalá ochrana transakcí před jejich nedokončením, nesprávným směrováním, neautorizovanou změnou předávaného datového obsahu, kompromitací, neautorizovaným duplikováním nebo opakováním.				

3.2.10. Kryptografické prostředky (VKB § 25)

KII	VIS			N	P	Z	NA
X	X	Pro používání kryptografické ochrany je(jsou) stanovena:					
X	X	odst. 1 a) 1.	Úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu.				
X	X	odst. 1 a) 2.	Pravidla kryptografické ochrany informací při přenosu po komunikačních sítích nebo při uložení na mobilní zařízení nebo vyměnitelné technické nosiče dat.				
X	X	odst. 1 b)	V souladu s bezpečnostními potřebami a výsledky hodnocení rizik jsou používány kryptografické prostředky, které zajistí ochranu důvěrnosti a integrity předávaných nebo ukládaných dat a prokázání odpovědnosti za provedené činnosti.				
X		odst. 2 a)	Pro používání kryptografických prostředků je stanoven systém správy klíčů, který zajistí generování, distribuci, ukládání, archivaci, změny, ničení, kontrolu a audit klíčů.				
X		odst. 2 b)	Jsou používány odolné kryptografické algoritmy a kryptografické klíče; v případě nesouladu s minimálními požadavky na kryptografické algoritmy uvedenými v příloze č. 3 k této vyhlášce řídí rizika spojená s tímto nesouladem.				

3.2.11. Nástroj pro zajišťování úrovně dostupnosti (VKB § 26)

KII	VIS			N	P	Z	NA
X	X	odst. 1	V souladu s bezpečnostními potřebami a výsledky hodnocení rizik je používán nástroj pro zajišťování úrovně dostupnosti informací.				
X		Je používán nástroj pro zajišťování úrovně dostupnosti informací, který zajišťuje:					
X		odst. 2 a)	Dostupnost informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury pro splnění cílů řízení kontinuity činností.				
X		odst. 2 b)	Odolnost informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury vůči kybernetickým bezpečnostním incidentům, které by mohly snížit dostupnost.				
X		odst. 2 c)	Zálohování důležitých technických aktiv informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury 1. využitím redundance v návrhu řešení a 2. zajištěním náhradních technických aktiv v určeném čase.				

3.2.12. Bezpečnost průmyslových a řídících systémů (VKB § 27)

KII	VIS			N	P	Z	NA
X		Pro bezpečnost průmyslových a řídících systémů, které jsou informačním systémem kritické informační infrastruktury nebo komunikačním systémem kritické informační infrastruktury anebo jsou jejich součástí, jsou používány nástroje, které zajišťují:					
X		a)	Omezení fyzického přístupu k síti a zařízením průmyslových a řídících systémů.				
X		b)	Omezení propojení a vzdáleného přístupu k síti průmyslových a řídících systémů.				
X		c)	Ochranu jednotlivých technických aktiv průmyslových a řídících systémů před využitím známých zranitelností.				
X		d)	Obnovení chodu průmyslových a řídících systémů po kybernetickém bezpečnostním incidentu.				

4. Struktura bezpečnostní dokumentace

Tato kapitola doplňuje Přílohu č. 4 k VKB. Obsahuje doporučený obsah bezpečnostní dokumentace pro správce kritické informační infrastruktury a významných informačních systémů. Struktura bezpečnostní dokumentace není striktně závazná, je možné použít strukturu jinou, důležitý je v tomto případě obsah dokumentace a soulad se zákonem o kybernetické bezpečnosti.

(1) Politika systému řízení bezpečnosti informací * **viz. *§ 3*, *§ 5***

a) Cíle, principy a potřeby řízení bezpečnosti informací.
b) Rozsah a hranice systému řízení bezpečnosti informací.
c) Pravidla a postupy pro řízení dokumentace.
d) Pravidla a postupy pro řízení zdrojů a provozu systému řízení bezpečnosti informací.
e) Pravidla a postupy pro provádění auditů kybernetické bezpečnosti.
f) Pravidla a postupy pro přezkoumání systému řízení bezpečnosti informací.
g) Pravidla a postupy pro nápravná opatření a zlepšování systému řízení bezpečnosti informací.

(2) Politika organizační bezpečnosti ** **viz. *§ 6***

a) Určení bezpečnostních rolí a jejich práv a povinností,
    1. práva a povinnosti manažera kybernetické bezpečnosti,
    2. práva a povinnosti architekta kybernetické bezpečnosti,
    3. práva a povinnosti auditora kybernetické bezpečnosti,
    4. práva a povinnosti garanta aktiv,
    5. práva a povinnosti výboru pro řízení kybernetické bezpečnosti.
b) Požadavky na oddělení odpovědností.

(3) Politika řízení dodavatelů ** **viz. *§ 7***

a) Pravidla a principy pro výběr dodavatelů.
b) Pravidla pro hodnocení rizik dodavatelů.
c) Náležitosti smlouvy o úrovni služeb a způsobů a úrovní realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti.
d) Pravidla pro provádění kontroly zavedení bezpečnostních opatření.
e) Pravidla pro hodnocení dodavatelů.

(4) Politika klasifikace aktiv ** **viz. *§ 8***

a) Identifikace, hodnocení a evidence primárních aktiv
    1. určení a evidence jednotlivých primárních aktiv včetně určení jejich garanta,
    2. hodnocení důležitosti primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti.
b) Identifikace, hodnocení a evidence podpůrných aktiv
    1. určení a evidence jednotlivých podpůrných aktiv včetně určení jejich garanta,
    2. určení vazeb mezi primárními a podpůrnými aktivy.
c) Pravidla ochrany jednotlivých úrovní aktiv
    1. způsoby rozlišování jednotlivých úrovní aktiv,
    2. pravidla pro manipulaci a evidenci aktiv podle úrovní aktiv,
    3. přípustné způsoby používání aktiv.
d) Způsoby spolehlivého smazání nebo ničení technických nosičů dat.

(5) Politika bezpečnosti lidských zdrojů ** **viz. *§ 9***

a) Pravidla rozvoje bezpečnostního povědomí a způsoby jeho hodnocení
    1. způsoby a formy poučení uživatelů,
    2. způsoby a formy poučení garantů aktiv,
    3. způsoby a formy poučení administrátorů,
    4. způsoby a formy poučení dalších osob zastávajících bezpečnostní role.
b) Bezpečnostní školení nových zaměstnanců.
c) Pravidla pro řešení případů porušení bezpečnostní politiky systému řízení bezpečnosti informací.
d) Pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice.
    1. vrácení svěřených aktiv a odebrání práv při ukončení pracovního vztahu,
    2. změna přístupových oprávnění při změně pracovní pozice.

(6) Politika řízení provozu a komunikací ** **viz. *§ 10***

a) Pravomoci a odpovědnosti spojené s bezpečným provozem.
b) Postupy bezpečného provozu.
c) Požadavky a standardy bezpečného provozu.
d) Řízení technických zranitelností.
e) Pravidla a omezení pro provádění auditů kybernetické bezpečnosti a bezpečnostních testů.

(7) Politika řízení přístupu ** **viz. *§ 11***

a) Princip minimálních oprávnění/potřeba znát (*need to know*).
b) Požadavky na řízení přístupu.
c) Životní cyklus řízení přístupu.
d) Řízení privilegovaných oprávnění.
e) Řízení přístupu pro mimořádné situace.
f) Pravidelné přezkoumání přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách.

(8) Politika bezpečného chování uživatelů * **viz. *§ 11***

a) Pravidla pro bezpečné nakládání s aktivy.
b) Bezpečné použití přístupového hesla.
c) Bezpečné použití elektronické pošty a přístupu na internet.
d) Bezpečný vzdálený přístup.
e) Bezpečné chování na sociálních sítích.
f) Bezpečnost ve vztahu k mobilním zařízením.

(9) Politika zálohování a obnovy ** **viz. *§ 10***

a) Požadavky na zálohování a obnovu.
b) Pravidla a postupy zálohování.
c) Pravidla bezpečného uložení záloh.
d) Pravidla a postupy obnovy.
e) Pravidla a postupy testování zálohování a obnovy.

(10) Politika bezpečného předávání a výměny informací ** **viz. *§ 10***

a) Pravidla a postupy pro ochranu předávaných informací.
b) Způsoby ochrany elektronické výměny informací.
c) Pravidla pro využívání kryptografické ochrany.

(11) Politika řízení technických zranitelností ** **viz. *§ 4*, *§ 5***

a) Pravidla pro omezení instalace programového vybavení,
b) Pravidla a postupy vyhledávání opravných programových balíčků,
c) Pravidla a postupy testování oprav programového vybavení,
d) Pravidla a postupy nasazení oprav programového vybavení.

(12) Politika bezpečného používání mobilních zařízení * **viz. *§ 5*, *§ 11***

a) Pravidla a postupy pro bezpečné používání mobilních zařízení.
b) Pravidla a postupy pro zajištění bezpečnosti zařízení, kterými orgán a osoba uvedená v § 3 písm. c) a d) zákona nedisponuje.

(13) Politika poskytování a nabývání licencí programového vybavení a informací * **viz. *§ 4*, *§ 5***

a) Pravidla a postupy nasazení programového vybavení a jeho evidence.
b) Pravidla a postupy pro kontrolu dodržování licenčních podmínek.

(14) Politika dlouhodobého ukládání a archivace informací * **viz. *§ 5*, *§ 25***

a) Pravidla a postupy archivace dokumentů a záznamů.
b) Ochrana archivovaných dokumentů a záznamů.
c) Politika přístupu k archivovaným dokumentům a záznamům.

(15) Politika ochrany osobních údajů * **viz. *§ 5*, *§ 8***

a) Charakteristika zpracovávaných osobních údajů.
b) Popis přijatých a provedených organizačních opatření pro ochranu osobních údajů.
c) Popis přijatých a provedených technických opatření pro ochranu osobních údajů.

(16) Politika fyzické bezpečnosti ** **viz. *§ 5*, *§ 16***

a) Pravidla pro ochranu objektů.
b) Pravidla pro kontrolu vstupu osob.
c) Pravidla pro ochranu zařízení.
d) Detekce narušení fyzické bezpečnosti.

(17) Politika bezpečnosti komunikační sítě ** **viz. *§ 17***

a) Pravidla a postupy pro zajištění bezpečnosti sítě.
b) Určení práv a povinností za bezpečný provoz sítě.
c) Pravidla a postupy pro řízení přístupů v rámci sítě.
d) Pravidla a postupy pro ochranu vzdáleného přístupu k síti.
e) Pravidla a postupy pro monitorování sítě a vyhodnocování provozních záznamů.

(18) Politika ochrany před škodlivým kódem * **viz. *§ 4*, *§ 20***

a) Pravidla a postupy pro ochranu komunikace mezi vnitřní a vnější sítí.
b) Pravidla a postupy pro ochranu serverů a sdílených datových uložišť.
c) Pravidla a postupy pro ochranu pracovních stanic.

(19) Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí **
viz.*§ 13*, *§ 22*

a) Pravidla a postupy nasazení nástroje pro detekci kybernetických bezpečnostních událostí.
b) Provozní postupy pro vyhodnocování a reagování na detekované kybernetické bezpečnostní události.
c) Pravidla a postupy pro optimalizaci nastavení nástroje pro detekci kybernetických bezpečnostních událostí.

(20) Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí **
viz. *§ 13*, *§ 23*

a) Pravidla a postupy pro evidenci a vyhodnocení kybernetických bezpečnostních událostí.
b) Pravidla a postupy pravidelné aktualizace pravidel pro vyhodnocení kybernetických bezpečnostních událostí.
c) Pravidla a postupy pro optimální nastavení bezpečnostních vlastností nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí.

(21) Politika bezpečného používání kryptografické ochrany ** **viz. *§ 25***

a) Úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu.
b) Pravidla kryptografické ochrany informací
    1. při přenosu po komunikačních sítích,
    2. při uložení na mobilní zařízení nebo vyměnitelný technický nosič dat,
c) Systém správy klíčů.

Poznámka:

* Očekávaná důvěrnost dokumentu je na úrovni střední podle stupnice uvedené v příloze č. 1 k VKB: Hodnocení a úroveň aktiv.

** Očekávaná důvěrnost dokumentu je na úrovni vysoká podle stupnice uvedené v příloze č. 1 k VKB: Hodnocení a úroveň aktiv.

5. Struktura další dokumentace

(1) Zpráva z auditu kybernetické bezpečnosti ** **viz. *§ 15***

[§ 28 odst. 1 písm. b)]

a) Cíle auditu kybernetické bezpečnosti.
b) Předmět auditu kybernetické bezpečnosti.
c) Kritéria auditu kybernetické bezpečnosti.
d) Identifikování týmu auditorů a osob, které se auditu kybernetické bezpečnosti zúčastnily.
e) Datum a místo, kde byly prováděny činnosti při auditu kybernetické bezpečnosti.
f) Zjištění z auditu kybernetické bezpečnosti.
g) Závěry auditu kybernetické bezpečnosti.

(2) Zpráva z přezkoumání systému řízení bezpečnosti informací **

a) Vyhodnocení opatření z předchozího přezkoumání systému řízení bezpečnosti informací,
b) Identifikace změn a okolností, které mohou mít vliv na systém řízení bezpečnosti informací.
c) Zpětná vazba o výkonnosti řízení bezpečnosti informací
    1. neshody a nápravná opatření,
    2. výsledky monitorování a měření,
    3. výsledky auditu,
    4. naplnění cílů bezpečnosti,
d) Výsledky hodnocení rizik a stav plánu zvládání rizik.
e) Identifikace možností pro neustálé zlepšování.
f) Doporučení potřebných rozhodnutí, stanovení opatření a odpovědných osob.

(3) Metodika pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik * **viz. *§ 4*, *§ 8***

a) Určení stupnice pro hodnocení primárních aktiv
    1. určení stupnice pro hodnocení úrovní důvěrnosti aktiv,
    2. určení stupnice pro hodnocení úrovní integrity aktiv,
    3. určení stupnice pro hodnocení úrovní dostupnosti aktiv.
b) Určení stupnice pro hodnocení rizik
    1. určení stupnice pro hodnocení úrovní dopadu,
    2. určení stupnice pro hodnocení úrovní hrozby,
    3. určení stupnice pro hodnocení úrovní zranitelnosti,
    4. určení stupnice pro hodnocení úrovní rizik,
c) Metody a přístupy pro zvládání rizik.
d) Způsoby schvalování přijatelných rizik.

(4) Zpráva o hodnocení aktiv a rizik ** **viz. *§ 4*, *§ 8***

a) Přehled primárních aktiv
    1. identifikace a popis primárních aktiv,
    2. určení garantů primárních aktiv,
    3. hodnocení primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti.
b) Přehled podpůrných aktiv (neplatí pro orgány a osoby uvedené v § 3 písm. e) zákona)
    1. identifikace a popis podpůrných aktiv,
    2. určení garantů podpůrných aktiv,
    3. určení vazeb mezi primárními a podpůrnými aktivy,
c) Identifikování a hodnocení rizik
    1. posouzení možných dopadů na aktiva,
    2. hodnocení existujících hrozeb,
    3. hodnocení existujících zranitelností, hodnocení existujících opatření,
    4. stanovení úrovně rizika, porovnání této úrovně s kritérii pro přijatelnost rizik,
    5. určení a schválení přijatelných rizik.

d) Zvládání rizik
    1. návrh způsobu zvládání rizik,
    2. návrh opatření a jejich realizace.

(5) Prohlášení o aplikovatelnosti * **viz. *§ 8***

a) Přehled vybraných bezpečnostních opatření včetně zdůvodnění jejich výběru a jejich vazby na identifikovaná rizika.
b) Přehled zavedených bezpečnostních opatření.

(6) Plán zvládání rizik ** **viz. *§ 8***

a) Obsah a cíle vybraných bezpečnostních opatření pro zvládání rizik.
b) Potřebné zdroje pro jednotlivá bezpečnostní opatření pro zvládání rizik.
c) Osoby odpovědné za jednotlivá bezpečnostní opatření pro zvládání rizik.
d) Termíny zavedení jednotlivých bezpečnostních opatření pro zvládání rizik.
e) Způsoby hodnocení úspěšnosti zavedení jednotlivých bezpečnostních opatření pro zvládání rizik.

(7) Plán rozvoje bezpečnostního povědomí * **viz. *§ 3*, *§ 6***

a) Obsah a termíny poučení uživatelů.
b) Obsah a termíny poučení garantů aktiv (neplatí pro orgány a osoby uvedené v § 3 písm. e) zákona).
c) Obsah a termíny poučení administrátorů (neplatí pro orgány a osoby uvedené v § 3 písm. e) zákona).
d) Obsah a termíny poučení dalších osob zastávajících bezpečnostní role.
e) Obsah a termíny poučení nových zaměstnanců.
f) Formy a způsoby hodnocení plánu.

(8) Zvládání kybernetických bezpečnostních incidentů ** **viz. *§ 13***

a) Definování kategorií kybernetického bezpečnostního incidentu.
b) Pravidla a postupy pro evidenci a zvládání jednotlivých kategorií kybernetických bezpečnostních incidentů.
c) Pravidla a postupy testování systému zvládání kybernetických bezpečnostních incidentů.
d) Pravidla a postupy pro vyhodnocení kybernetických bezpečnostních incidentů a pro zlepšování kybernetické bezpečnosti.

(9) Strategie řízení kontinuity činností ** **viz. *§ 14***

a) Práva a povinnosti zúčastněných osob.
b) Cíle řízení kontinuity činností
    1. minimální úroveň poskytovaných služeb,
    2. doba obnovení chodu,
    3. bod obnovení chodu.
c) Strategie řízení kontinuity činností pro naplnění cílů kontinuity.
d) Způsoby hodnocení dopadů kybernetických bezpečnostních incidentů na kontinuitu a posuzování souvisejících rizik.
e) Určení a obsah potřebných plánů kontinuity.
f) Postupy pro realizaci opatření vydaných Národním bezpečnostním úřadem.

(10) Přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků *

a) Přehled obecně závazných právních předpisů.
b) Přehled vnitřních předpisů a jiných předpisů.
c) Přehled smluvních závazků.

Poznámka:
* Očekávaná důvěrnost dokumentu je na úrovni střední podle stupnice uvedené v příloze č. 1 k VKB: Hodnocení a úroveň aktiv.
** Očekávaná důvěrnost dokumentu je na úrovni vysoká podle stupnice uvedené v příloze č. 1 k VKB: Hodnocení a úroveň aktiv.

6. Seznam použitých zkratek

IS	informační systém
ISMS	systém řízení bezpečnosti informací (*Information Security Management System*)
KII	kritická informační infrastruktura
KS	komunikační systém
VIS	významný informační systém
VKB	vyhláška o kybernetické bezpečnosti
ZKB	zákon o kybernetické bezpečnosti

7. Doporučené informační zdroje

- JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. 3., aktualiz. vyd. Praha: Česká pobočka AFCEA, 2015, 200 s. ISBN 978-80-7251-436-6.
- Česká republika. Zákon č. 181 ze dne 23. července 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů České republiky. 2014. - www.nbu.cz/cs/pravni-predpisy/zakon-o-kyberneticke-bezpecnosti-a-o-zmene-souvisejicich-zakonu-zakon-o-kyberneticke-bezpecnosti/*Česká republika.
- Vyhláška č. 316 ze dne 19. prosince 2014 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). In: *Sbírka zákonů České republiky. 2014.* - www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/provadeci-pravni-predpisy-k-zakonu-c-1812014-sb-o-kyberneticke-bezpecnosti-a-o-zmene-souvisejicich-zakonu/
- ČSN ISO/IEC 27001. *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací* - Požadavky. Praha: Český normalizační institut.
- DOUCEK, Petr. *Řízení bezpečnosti informací*: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.
- DOUCEK, Petr, Luděk NOVÁK a Vlasta SVATÁ. *Řízení bezpečnosti informací*. 1. vyd. Praha: Professional Publishing, 2008, 239 s. ISBN 978-80-86946-88-7.

Verze dokumentu

datum	verze	změněno (jméno)	změna
1. 5. 2015	1.0	Konečný	Základní verze dokumentu
18. 11. 2015	2.0	Konečný	Do tabulek přidán sloupec „NA“ (neaplikovatelné)
1. 2. 2015	2.1	Rybáková	Oprava gramatiky