82

VYHLÁŠKA
ze dne 21. května 2018

o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

Národní úřad pro kybernetickou a informační bezpečnost stanoví podle § 28 odst. 2 písm. a) až d) a f) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb. a zákona č. 205/2017 Sb., (dále jen „zákon“):

ČÁST PRVNÍ
ÚVODNÍ USTANOVENÍ

§ 1
Předmět úpravy

Tato vyhláška zapracovává příslušný předpis Evropské unie[1]) a pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury, významný informační systém, informační systém základní služby anebo informační systém nebo síť elektronických komunikací, které využívá poskytovatel digitálních služeb, (dále jen „informační a komunikační systém“) upravuje

a) obsah a strukturu bezpečnostní dokumentace,
b) obsah a rozsah bezpečnostních opatření,
c) typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů,
d) náležitosti a způsob hlášení kybernetického bezpečnostního incidentu,
e) náležitosti oznámení o provedení reaktivního opatření a jeho výsledku,
f) vzor oznámení kontaktních údajů a jeho formu a
g) způsob likvidace dat, provozních údajů, informací a jejich kopií.

§ 2

Vymezení pojmů

Pro účely této vyhlášky se rozumí

a) administrátorem osoba zajišťující správu, provoz, použití, údržbu a bezpečnost technického aktiva,

b) akceptovatelným rizikem riziko, které je přijatelné pro orgán nebo osobu, které jsou povinny zavést bezpečnostní opatření podle zákona, (dále jen „povinná osoba“) a není nutné jej zvládat pomocí dalších bezpečnostních opatření,

c) bezpečnostní politikou soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv,

d) hodnocením rizik celkový proces identifikace, analýzy a vyhodnocení rizik,

e) hrozbou potenciální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, která může způsobit škodu,

f) podpůrným aktivem technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému,

g) primárním aktivem informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém,

h) rizikem možnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu,

i) řízením rizik činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik,

j) systémem řízení bezpečnosti informací část systému řízení povinné osoby založená na přístupu k rizikům informačního a komunikačního systému, která stanoví způsob ustavení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací a dat,

k) technickým aktivem takové technické vybavení, komunikační prostředky a programové vybavení informačního a komunikačního systému a objekty, ve kterých jsou tyto systémy umístěny, jejichž selhání může mít dopad na informační a komunikační systém,

l) uživatelem fyzická nebo právnická osoba anebo orgán veřejné moci, které využívají aktiva,

m) vrcholovým vedením osoba nebo skupina osob, které řídí povinnou osobu, nebo statutární orgán povinné osoby,

n) významným dodavatelem provozovatel informačního nebo komunikačního systému (dále jen „provozovatel“) a každý, kdo s povinnou osobou vstupuje do právního vztahu, který je významný z hlediska bezpečnosti informačního a komunikačního systému,

o) významnou změnou změna, která má nebo může mít vliv na kybernetickou bezpečnost a představuje vysoké riziko,

p) zranitelností slabé místo aktiva nebo slabé místo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami.

ČÁST DRUHÁ
BEZPEČNOSTNÍ OPATŘENÍ

HLAVA I
ORGANIZAČNÍ OPATŘENÍ

§ 3
Systém řízení bezpečnosti informací

Povinná osoba v rámci systému řízení bezpečnosti informací

a) stanoví s ohledem na požadavky dotčených stran a organizační bezpečnost rozsah systému řízení bezpečnosti informací, ve kterém určí organizační části a aktiva, jichž se systém řízení bezpečnosti informací týká,
b) stanoví cíle systému řízení bezpečnosti informací,
c) pro stanovený rozsah systému řízení bezpečnosti informací na základě cílů systému řízení bezpečnosti informací, bezpečnostních potřeb a hodnocení rizik zavede přiměřená bezpečnostní opatření,
d) řídí rizika podle § 5,
e) vytvoří a schválí bezpečnostní politiku v oblasti systému řízení bezpečnosti informací, která obsahuje hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací, a na základě bezpečnostních potřeb a výsledků hodnocení rizik stanoví bezpečnostní politiku v dalších oblastech podle § 30 a zavede přiměřená bezpečnostní opatření,
f) zajistí provedení auditu kybernetické bezpečnosti u informačního a komunikačního systému (dále jen „audit kybernetické bezpečnosti“) podle § 16,
g) zajistí pravidelné vyhodnocování účinnosti systému řízení bezpečnosti informací, které obsahuje hodnocení stavu systému řízení bezpečnosti informací včetně revize hodnocení rizik, posouzení výsledků provedených auditů kybernetické bezpečnosti a dopadů kybernetických bezpečnostních incidentů na systém řízení bezpečnosti informací,
h) průběžně identifikuje a následně podle § 11 řídí významné změny, které patří do rozsahu systému řízení bezpečnosti informací,
i) aktualizuje systém řízení bezpečnosti informací a příslušnou dokumentaci na základě zjištění auditů kybernetické bezpečnosti, výsledků vyhodnocení účinnosti systému řízení bezpečnosti informací a v souvislosti s prováděnými významnými změnami a
j) řídí provoz a zdroje systému řízení bezpečnosti informací a zaznamenává činnosti spojené se systémem řízení bezpečnosti informací a řízením rizik.

§ 4
Řízení aktiv

(1) Povinná osoba v rámci řízení aktiv

a) stanoví metodiku pro identifikaci aktiv,
b) stanoví metodiku pro hodnocení aktiv alespoň v rozsahu uvedeném v příloze č. 1 k této vyhlášce,

c) identifikuje a eviduje aktiva,
d) určí a eviduje garanty aktiv,
e) hodnotí a eviduje primární aktiva z hlediska důvěrnosti, integrity a dostupnosti a zařadí je do jednotlivých úrovní podle písmene b),
f) určí a eviduje vazby mezi primárními a podpůrnými aktivy a hodnotí důsledky závislostí mezi primárními a podpůrnými aktivy,
g) hodnotí podpůrná aktiva a zohledňuje přitom zejména vzájemné závislosti podle písmene f),
h) na základě hodnocení aktiv stanovuje a zavádí pravidla ochrany nutná pro zabezpečení jednotlivých úrovní aktiv,
i) stanoví přípustné způsoby používání aktiv a pravidla pro manipulaci s aktivy s ohledem na úroveň aktiv, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv, a
j) určí způsob likvidace dat, provozních údajů, informací a jejich kopií nebo likvidaci technických nosičů dat s ohledem na úroveň aktiv v souladu s přílohou č. 4 k této vyhlášce.

(2) Při hodnocení důležitosti primárních aktiv je třeba posoudit alespoň
a) rozsah a důležitost osobních údajů, zvláštních kategorií osobních údajů nebo obchodního tajemství,
b) rozsah dotčených právních povinností nebo jiných závazků,
c) rozsah narušení vnitřních řídicích a kontrolních činností,
d) poškození veřejných, obchodních nebo ekonomických zájmů a možné finanční ztráty,
e) dopady na poskytování důležitých služeb,
f) rozsah narušení běžných činností,
g) dopady na zachování dobrého jména nebo ochranu dobré pověsti,
h) dopady na bezpečnost a zdraví osob,
i) dopady na mezinárodní vztahy a
j) dopady na uživatele informačního a komunikačního systému.

§ 5

Řízení rizik

(1) Povinná osoba v rámci řízení rizik v návaznosti na § 4
a) stanoví metodiku pro hodnocení rizik, včetně stanovení kritérií pro akceptovatelnost rizik,
b) s ohledem na aktiva identifikuje relevantní hrozby a zranitelnosti; přitom zvažuje zejména kategorie hrozeb a zranitelností uvedených v příloze č. 3 k této vyhlášce,
c) provádí hodnocení rizik v pravidelných intervalech podle odstavce 2 a při významných změnách,
d) při hodnocení rizik zohlední relevantní hrozby a zranitelnosti a posoudí možné dopady na aktiva; tato rizika hodnotí alespoň v rozsahu přílohy č. 2 k této vyhlášce,
e) zpracuje zprávu o hodnocení rizik,

f) zpracuje na základě bezpečnostních potřeb a výsledků hodnocení rizik prohlášení o aplikovatelnosti, které obsahuje přehled bezpečnostních opatření požadovaných touto vyhláškou, která

   1. nebyla aplikována, včetně odůvodnění,
   2. byla aplikována, včetně způsobu plnění,

g) zpracuje a zavede plán zvládání rizik, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání jednotlivých rizik, určení osoby zajišťující prosazování bezpečnostních opatření pro zvládání rizik, potřebné finanční, technické, lidské a informační zdroje, termín jejich zavedení, popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními a způsob realizace bezpečnostních opatření,

h) při hodnocení rizik a v plánu zvládání rizik zohlední

   1. významné změny,
   2. změny rozsahu systému řízení bezpečnosti informací,
   3. opatření podle § 11 zákona a
   4. kybernetické bezpečnostní incidenty, včetně dříve řešených, a

i) v souladu s plánem zvládání rizik zavádí bezpečnostní opatření.

(2) Povinná osoba uvedená v § 3 písm. c), d) a f) zákona provádí hodnocení rizik alespoň jednou ročně a povinná osoba uvedená v § 3 písm. e) zákona alespoň jednou za tři roky.

(3) Řízení rizik může být zajištěno i jinými způsoby, než jak je stanoveno v odstavci 1 písm. d), pokud povinná osoba zabezpečí, že použitá opatření zajistí stejnou nebo vyšší úroveň procesu řízení rizik.

§ 6

Organizační bezpečnost

(1) Povinná osoba s ohledem na systém řízení bezpečnosti informací

a) zajistí stanovení bezpečnostní politiky a cílů systému řízení bezpečnosti informací podle § 3 slučitelných se strategickým směřováním povinné osoby,

b) zajistí integraci systému řízení bezpečnosti informací do procesů povinné osoby,

c) zajistí dostupnost zdrojů potřebných pro systém řízení bezpečnosti informací,

d) informuje zaměstnance o významu systému řízení bezpečnosti informací a významu dosažení shody s jeho požadavky se všemi dotčenými stranami,

e) zajistí podporu k dosažení zamýšlených výstupů systému řízení bezpečnosti informací,

f) vede zaměstnance k rozvíjení efektivity systému řízení bezpečnosti informací a podporuje je při tomto rozvíjení,

g) prosazuje neustálé zlepšování systému řízení bezpečnosti informací,

h) podporuje osoby zastávající bezpečnostní role při prosazování kybernetické bezpečnosti v oblastech jejich odpovědnosti,

i) zajistí stanovení pravidel pro určení administrátorů a osob, které budou zastávat bezpečnostní role,

j) zajistí, aby byla zachována mlčenlivost administrátorů a osob zastávajících bezpečnostní role,

k) pro osoby zastávající bezpečnostní role zajistí příslušné pravomoci a zdroje včetně rozpočtových prostředků k naplňování jejich rolí a plnění souvisejících úkolů a

l) zajistí testování plánů kontinuity činností, obnovy a procesů spojených se zvládáním kybernetických bezpečnostních incidentů.

(2) Povinná osoba v rámci systému řízení bezpečnosti informací určí složení výboru pro řízení kybernetické bezpečnosti a bezpečnostní role a jejich práva a povinnosti související se systémem řízení bezpečnosti informací.

(3) Povinná osoba uvedená v § 3 písm. c), d) a f) zákona určí osobu, která bude zastávat bezpečnostní roli

a) manažera kybernetické bezpečnosti,

b) architekta kybernetické bezpečnosti,

c) garanta aktiva a

d) auditora kybernetické bezpečnosti.

(4) Povinná osoba uvedená v § 3 písm. e) zákona určí role manažera kybernetické bezpečnosti a garanta aktiva. Ostatní bezpečnostní role podle odstavce 3 určí přiměřeně vzhledem k rozsahu a potřebám systému řízení bezpečnosti informací.

(5) Povinná osoba uvedená v § 3 písm. c), d) a f) zákona zajistí zastupitelnost bezpečnostních rolí uvedených v odstavci 3 písm. a) a b).

(6) Povinná osoba uvedená v § 3 písm. e) zákona zajistí zastupitelnost bezpečnostní role manažera kybernetické bezpečnosti.

(7) Výbor pro řízení kybernetické bezpečnosti je tvořen osobami s příslušnými pravomocemi a odbornou způsobilostí pro celkové řízení a rozvoj systému řízení bezpečnosti informací a osobami významně se podílejícími na řízení a koordinaci činností spojených s kybernetickou bezpečností, jehož členem musí být alespoň jeden zástupce vrcholového vedení nebo jím pověřená osoba a manažer kybernetické bezpečnosti. Povinná osoba u výboru pro řízení kybernetické bezpečnosti přihlédne k doporučením uvedeným v příloze č. 6 k této vyhlášce.

§ 7

Bezpečnostní role

(1) Manažer kybernetické bezpečnosti

a) je bezpečnostní role odpovědná za systém 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

1. po dobu nejméně tří let, nebo
2. po dobu jednoho roku, pokud absolvovala studium na vysoké škole,

b) odpovídá za pravidelné informování vrcholového vedení o

1. činnostech vyplývajících z rozsahu jeho odpovědnosti a
2. stavu systému řízení bezpečnosti informací a

c) nesmí být pověřen výkonem rolí odpovědných za provoz informačního a komunikačního systému.

(2) Architekt kybernetické bezpečnosti je bezpečnostní role odpovědná za zajištění návrhu implementace bezpečnostních opatření tak, aby byla zajištěna bezpečná architektura informačního a komunikačního systému, 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 architektury bezpečnosti

a) po dobu nejméně tří let, nebo

b) po dobu jednoho roku, pokud absolvovala studium na vysoké škole.

(3) Garant aktiva je bezpečnostní role odpovědná za zajištění rozvoje, použití a bezpečnost aktiva.

(4) Auditor kybernetické bezpečnosti

a) je bezpečnostní role odpovědná za provádění 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

1. po dobu nejméně tří let, nebo
2. po dobu jednoho roku, pokud absolvovala studium na vysoké škole,

b) zaručuje, že provedení auditu kybernetické bezpečnosti je nestranné, a

c) nesmí být pověřen výkonem jiných bezpečnostních rolí.

(5) Povinná osoba při určování osob zastávajících bezpečnostní role přihlédne k doporučením uvedeným v příloze č. 6 k této vyhlášce.

§ 8

Řízení dodavatelů

(1) Povinná osoba

a) stanoví pravidla pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací,

b) vede evidenci svých významných dodavatelů,

c) prokazatelně písemně informuje své významné dodavatele o jejich evidenci podle písmene b),

d) seznamuje své dodavatele s pravidly podle písmene a) a vyžaduje plnění těchto pravidel,

e) řídí rizika spojená s dodavateli,

f) v souvislosti s řízením rizik spojených s významnými dodavateli zajistí, aby smlouvy uzavírané s významnými dodavateli obsahovaly relevantní oblasti uvedené v příloze č. 7 k této vyhlášce, a

g) pravidelně přezkoumává plnění smluv s významnými dodavateli z hlediska systému řízení bezpečnosti informací.

(2) Povinná osoba u významných dodavatelů dále

a) v rámci výběrového řízení a před uzavřením smlouvy provádí hodnocení rizik souvisejících s plněním předmětu výběrového řízení přiměřeně podle přílohy č. 2 k této vyhlášce,

b) v rámci uzavíraných smluvních vztahů stanoví způsoby a úrovně realizace bezpečnostních opatření a určí obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření,

c) provádí pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných plnění pomocí vlastních zdrojů nebo pomocí třetí strany a

d) v reakci na rizika a zjištěné nedostatky zajistí jejich řešení.

(3) Náležitosti prokazatelného informování podle odstavce 1 písm. c) jsou

a) identifikace správce nebo provozovatele,

b) identifikace informačního a komunikačního systému,

c) identifikace významného dodavatele,

d) vyrozumění o skutečnosti, že dodavatel je pro správce významným dodavatelem, a popřípadě také o tom, že významný dodavatel je zároveň provozovatelem, a

e) obsah pravidel podle odstavce 1 písm. a).

(4) Povinná osoba uvedená v § 3 písm. c) až f) zákona, která je provozovatelem a byla prokazatelně informována podle odstavce 1 písm. c), hlásí kontaktní údaje formou uvedenou v § 34.

§ 9

Bezpečnost lidských zdrojů

(1) Povinná osoba v rámci řízení bezpečnosti lidských zdrojů

a) s ohledem na stav a potřeby systému řízení bezpečnosti informací stanoví plán rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí a který obsahuje formu, obsah a rozsah

1. poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice a
2. potřebných teoretických i praktických školení uživatelů, administrátorů a osob zastávajících bezpečnostní role,

b) určí osoby odpovědné za realizaci jednotlivých činností, které jsou v plánu uvedeny,

c) v souladu s plánem rozvoje bezpečnostního povědomí zajistí poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení,

d) pro osoby zastávající bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí zajistí pravidelná odborná školení, přičemž vychází z aktuálních potřeb povinné osoby v oblasti kybernetické bezpečnosti,

e) v souladu s plánem rozvoje bezpečnostního povědomí zajistí pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní,

f) zajistí kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role,

g) v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role zajistí předání odpovědností,

h) hodnotí účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených se zlepšováním bezpečnostního povědomí a

i) určí pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.

(2) Povinná osoba vede o školení podle odstavce 1 přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.

§ 10

Řízení provozu a komunikací

(1) Povinná osoba v rámci řízení provozu a komunikací zajišťuje bezpečný provoz informačního a komunikačního systému a stanoví provozní pravidla a postupy, které obsahují zejména

a) práva a povinnosti administrátorů, uživatelů a osob zastávajících bezpečnostní role,
b) postupy pro spuštění a ukončení chodu systému, pro restart nebo obnovení chodu systému po selhání a pro ošetření chybových stavů nebo mimořádných jevů,
c) postupy pro sledování kybernetických bezpečnostních událostí a opatření pro ochranu přístupu k záznamům o těchto událostech,
d) pravidla a postupy pro ochranu před škodlivým kódem,
e) řízení technických zranitelností,
f) spojení na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory,
g) postupy řízení a schvalování provozních změn,
h) postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů,
i) pravidla a postupy pro ochranu informací a dat v průběhu celého životního cyklu,
j) pravidla a postupy pro instalaci technických aktiv,
k) provádění pravidelného zálohování a kontroly použitelnosti provedených záloh a
l) pravidla a postupy pro zajištění bezpečnosti síťových služeb.

(2) Povinná osoba v rámci řízení provozu a komunikací dodržuje pravidla a postupy stanovené podle odstavce 1 a tato pravidla a postupy aktualizuje v souvislosti s prováděnými nebo plánovanými změnami.

(3) Povinná osoba zajistí oddělení vývojového, testovacího a provozního prostředí.

§ 11

Řízení změn

(1) Povinná osoba v rámci řízení změn u informačního a komunikačního systému

a) přezkoumává možné dopady změn a
b) určuje významné změny.

(2) Povinná osoba u významných změn

a) dokumentuje jejich řízení,
b) provádí analýzu rizik,
c) přijímá opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami,
d) aktualizuje bezpečnostní politiku a bezpečnostní dokumentaci,

e) zajistí jejich testování a

f) zajistí možnost navrácení do původního stavu.

(3) Povinná osoba uvedená v § 3 písm. c), d) a f) zákona na základě výsledků analýzy rizik podle odstavce 2 písm. b) rozhoduje o provedení penetračního testování nebo testování zranitelností; pokud rozhodne o provedení penetračního testování nebo testování zranitelností, postupuje podle § 25 odst. 1 a reaguje na zjištěné nedostatky.

(4) Povinná osoba uvedená v § 3 písm. e) zákona se řídí požadavky podle odstavce 3 přiměřeně.

§ 12

Řízení přístupu

(1) Povinná osoba na základě provozních a bezpečnostních potřeb řídí přístup k informačnímu a komunikačnímu systému a přijímá opatření, která slouží k zajištění ochrany údajů, které jsou používány pro přihlášení podle § 19 a 20, a která brání ve zneužití těchto údajů neoprávněnou osobou.

(2) Povinná osoba dále v rámci řízení přístupu k informačnímu a komunikačnímu systému

a) řídí přístup na základě skupin a rolí,

b) přidělí každému uživateli a administrátorovi přistupujícímu k informačnímu a komunikačnímu systému přístupová práva a oprávnění a jedinečný identifikátor,

c) řídí identifikátory, přístupová práva a oprávnění aplikací a technických účtů,

d) zavádí bezpečnostní opatření pro řízení přístupu zařízení k prostředkům informačního a komunikačního systému,

e) zavádí bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení a jiných technických zařízení, popřípadě i bezpečnostní opatření spojená s využitím technických zařízení, která povinná osoba nemá ve své správě,

f) omezí přidělování privilegovaných oprávnění na úroveň nezbytně nutnou k výkonu náplně práce,

g) omezí a kontroluje používání programových prostředků, které mohou být schopné překonat systémové nebo aplikační kontroly,

h) přiděluje a odebírá přístupová oprávnění v souladu s politikou řízení přístupu,

i) provádí pravidelné přezkoumání nastavení veškerých přístupových oprávnění včetně rozdělení do přístupových skupin a rolí,

j) využívá nástroj pro správu a ověřování identity podle § 19 a nástroj pro řízení přístupových oprávnění podle § 20,

k) prosazuje, aby uživatelé při používání privátních autentizačních informací dodržovali stanovené postupy,

l) zajistí odebrání nebo změnu přístupových oprávnění při změně pozice nebo zařazení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role,

m) zajistí odebrání nebo změnu přístupových oprávnění při ukončení nebo změně smluvního vztahu a

n) dokumentuje přidělování a odebírání přístupových oprávnění.

§ 13

Akvizice, vývoj a údržba

Povinná osoba v souvislosti s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního systému

a) řídí rizika podle § 5,
b) řídí významné změny podle § 11,
c) stanoví bezpečnostní požadavky,
d) zahrne bezpečnostní požadavky do projektu akvizice, vývoje a údržby,
e) zajistí bezpečnost vývojového a testovacího prostředí a zajistí ochranu používaných testovacích dat,
f) provádí bezpečnostní testování významných změn před jejich zavedením do provozu a
g) plní požadavek podle § 19 odst. 3, je-li cílem provedení akvizice nebo vývoje nástroj pro správu a ověřování identity.

§ 14

Zvládání kybernetických bezpečnostních událostí a incidentů

(1) Povinná osoba v rámci zvládání kybernetických bezpečnostních událostí a incidentů

a) zavede proces detekce a vyhodnocování kybernetických bezpečnostních událostí a zvládání kybernetických bezpečnostních incidentů,
b) přidělí odpovědnosti a stanoví postupy pro
    1. detekci a vyhodnocování kybernetických bezpečnostních událostí a incidentů a
    2. koordinaci a zvládání kybernetických bezpečnostních incidentů,
c) definuje a aplikuje postupy pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu,
d) zajistí detekci kybernetických bezpečnostních událostí,
e) při detekci kybernetických bezpečnostních událostí se dále řídí § 22 a 23,
f) zajistí, že uživatelé, administrátoři, osoby zastávající bezpečnostní role, další zaměstnanci a dodavatelé budou oznamovat neobvyklé chování informačního a komunikačního systému a podezření na jakékoliv zranitelnosti,
g) zajistí posuzování kybernetických bezpečnostních událostí, při kterém musí být rozhodnuto, zda mají být klasifikovány jako kybernetické bezpečnostní incidenty podle § 31,
h) zajistí zvládání kybernetických bezpečnostních incidentů podle stanovených postupů,
i) přijímá opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu,
j) hlásí kybernetické bezpečnostní incidenty podle § 32,
k) vede záznamy o kybernetických bezpečnostních incidentech a o jejich zvládání,
l) prošetří a určí příčiny kybernetického bezpečnostního incidentu a
m) vyhodnotí účinnost řešení kybernetického bezpečnostního incidentu a na základě vyhodnocení stanoví nutná bezpečnostní opatření, popřípadě aktualizuje stávající bezpečnostní opatření k zamezení opakování řešeného kybernetického bezpečnostního incidentu.

(2) Povinná osoba uvedená v § 3 písm. c), d) a f) zákona dále při detekci kybernetických bezpečnostních událostí používá nástroj podle § 24.

§ 15

Řízení kontinuity činností

Povinná osoba v rámci řízení kontinuity činností

a) stanoví práva a povinnosti administrátorů a osob zastávajících bezpečnostní role,

b) pomocí hodnocení rizik a analýzy dopadů vyhodnotí a dokumentuje možné dopady kybernetických bezpečnostních incidentů a posoudí možná rizika související s ohrožením kontinuity činností,

c) na základě výstupů hodnocení rizik a analýzy dopadů podle písmene b) stanoví cíle řízení kontinuity činností formou určení

1. minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu informačního a komunikačního systému,
2. doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačního a komunikačního systému, a
3. bodu obnovení dat jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání,

d) stanoví politiku řízení kontinuity činností, která obsahuje naplnění cílů podle písmene c),

e) vypracuje, aktualizuje a pravidelně testuje plány kontinuity činností a havarijní plány související s provozováním informačního a komunikačního systému a souvisejících služeb a

f) realizuje opatření pro zvýšení odolnosti informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům a omezením dostupnosti a vychází při tom z požadavků podle § 27.

§ 16

Audit kybernetické bezpečnosti

(1) Povinná osoba v rámci auditu kybernetické bezpečnosti

a) provádí a dokumentuje audit dodržování bezpečnostní politiky, včetně přezkoumání technické shody, a výsledky auditu zohlední v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik a

b) posuzuje soulad bezpečnostních opatření s nejlepší praxí, právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k informačnímu a komunikačnímu systému a určí případná nápravná opatření pro zajištění souladu.

(2) Audit podle odstavce 1 je prováděn

a) při významných změnách, v rámci jejich rozsahu,

b) v pravidelných intervalech alespoň po 3 letech v případě povinné osoby uvedené v § 3 písm. e) zákona a

c) v pravidelných intervalech alespoň po 2 letech v případě povinné osoby neuvedené v písmenu b).

(3) Není-li v odůvodněných případech možné provést audit v intervalech podle odstavce 2 písm. b) a c) v celém rozsahu, je možné audit provádět průběžně po systematických celcích. V takovém případě je nutno audit v celém rozsahu provést nejpozději do 5 let.

(4) Audit kybernetické bezpečnosti musí být prováděn osobou vyhovující podmínkám stanoveným v § 7 odst. 4, která nezávisle hodnotí správnost a účinnost zavedených bezpečnostních opatření.

(5) Povinná osoba, která je současně provozovatelem, předkládá výsledky auditu kybernetické bezpečnosti správci daného informačního a komunikačního systému.

HLAVA II
TECHNICKÁ OPATŘENÍ

§ 17

Fyzická bezpečnost

Povinná osoba v rámci fyzické bezpečnosti

a) předchází poškození, krádeži nebo zneužití aktiv nebo přerušení poskytování služeb informačního a komunikačního systému,

b) stanoví fyzický bezpečnostní perimetr ohraničující oblast, ve které jsou uchovávány a zpracovávány informace a umístěna technická aktiva informačního a komunikačního systému, a

c) u fyzického bezpečnostního perimetru stanoveného podle písmene b) přijme nezbytná opatření a uplatňuje prostředky fyzické bezpečnosti

   1. k zamezení neoprávněnému vstupu,
   2. k zamezení poškození a neoprávněným zásahům a
   3. pro zajištění ochrany na úrovni objektů a v rámci objektů.

§ 18

Bezpečnost komunikačních sítí

Povinná osoba pro ochranu bezpečnosti komunikační sítě zahrnuté v rozsahu podle § 3 písm. c)

a) zajistí segmentaci komunikační sítě,

b) zajistí řízení komunikace v rámci komunikační sítě a perimetru komunikační sítě,

c) pomocí kryptografie zajistí důvěrnost a integritu dat při vzdáleném přístupu, vzdálené správě nebo při přístupu do komunikační sítě pomocí bezdrátových technologií,

d) aktivně blokuje nežádoucí komunikaci a

e) pro zajištění segmentace sítě a pro řízení komunikace mezi jejími segmenty využívá nástroj, který zajistí ochranu integrity komunikační sítě.

§ 19

Správa a ověřování identit

(1) Povinná osoba používá nástroj pro správu a ověření identity uživatelů, administrátorů a aplikací informačního a komunikačního systému.

(2) Nástroj pro správu a ověření identity uživatelů, administrátorů a aplikací zajišťuje

a) ověření identity před zahájením aktivit v informačním a komunikačním systému,

b) řízení počtu možných neúspěšných pokusů o přihlášení,

c) odolnost uložených nebo přenášených autentizačních údajů proti neoprávněnému odcizení a zneužití,

d) ukládání autentizačních údajů ve formě odolné proti offline útokům,

e) opětovné ověření identity po určené době nečinnosti,

f) dodržení důvěrnosti autentizačních údajů při obnově přístupu a

g) centralizovanou správu identit.

(3) Povinná osoba pro ověření identity uživatelů, administrátorů a aplikací využívá autentizační mechanizmus, který není založený pouze na použití identifikátoru účtu a hesla, nýbrž na vícefaktorové autentizaci s nejméně dvěma různými typy faktorů.

(4) Do doby splnění požadavku podle odstavce 3 musí nástroj pro ověření identity uživatelů, administrátorů a aplikací, používat autentizaci pomocí kryptografických klíčů a zaručit obdobnou úroveň bezpečnosti.

(5) Do doby splnění požadavků podle odstavce 3 nebo 4 musí nástroj pro ověření identity uživatelů, administrátorů a aplikací, který používá k autentizaci identifikátor účtu a heslo, vynucovat pravidla

a) délky hesla alespoň

1. 12 znaků u uživatelů a
2. 17 znaků u administrátorů a aplikací,

b) umožňující zadat heslo o délce alespoň 64 znaků,

c) neomezující použití malých a velkých písmen, číslic a speciálních znaků,

d) umožňující uživatelům změnu hesla, přičemž období mezi dvěma změnami hesla nesmí být kratší než 30 minut,

e) neumožňující uživatelům a administrátorům

1. zvolit si nejčastěji používaná hesla,
2. tvořit hesla na základě mnohonásobně opakujících se znaků, přihlašovacího jména, e-mailu, názvu systému nebo obdobným způsobem a
3. opětovné použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel a

f) pro povinnou změnu hesla v intervalu maximálně po 18 měsících, přičemž toto pravidlo se nevztahuje na účty sloužící k obnově systému v případě havárie.

(6) Povinná osoba v případě používání autentizace pouze účtem a heslem dále

a) vynutí bezodkladnou změnu výchozího hesla po jeho prvním použití,

b) bezodkladně zneplatní heslo sloužící k obnovení přístupu po jeho prvním použití nebo uplynutím nejvýše 60 minut od jeho vytvoření a

c) povinně zahrne pravidla tvorby bezpečných hesel do plánu rozvoje bezpečnostního povědomí podle § 9.

§ 20

Řízení přístupových oprávnění

Povinná osoba používá centralizovaný nástroj pro řízení přístupových oprávnění, kterým zajistí řízení oprávnění

a) pro přístup k jednotlivým aktivům informačního a komunikačního systému a
b) pro čtení dat, zápis dat a změnu oprávnění.

§ 21

Ochrana před škodlivým kódem

(1) Povinná osoba uvedená v § 3 písm. c), d) a f) zákona v rámci ochrany před škodlivým kódem

a) s ohledem na důležitost aktiv zajišťuje použití nástroje pro nepřetržitou automatickou ochranu

1. koncových stanic,
2. mobilních zařízení,
3. serverů,
4. datových úložišť a výměnných datových nosičů,
5. komunikační sítě a prvků komunikační sítě a
6. obdobných zařízení,

b) monitoruje a řídí používání výměnných zařízení a datových nosičů,
c) řídí automatické spouštění obsahu výměnných zařízení a datových nosičů,
d) řídí oprávnění ke spouštění kódu a
e) provádí pravidelnou a účinnou aktualizaci nástroje pro ochranu před škodlivým kódem.

(2) Povinná osoba uvedená v § 3 písm. e) zákona postupuje podle odstavce 1 přiměřeně.

§ 22

Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů

(1) Povinná osoba

a) zaznamenává bezpečnostní a potřebné provozní události důležitých aktiv informačního a komunikačního systému a
b) na základě hodnocení důležitosti aktiv aktualizuje rozsah aktiv, u kterých je zaznamenávání bezpečnostních a provozních událostí prováděno.

(2) Povinná osoba pro zaznamenávání bezpečnostních a provozních událostí podle odstavce 1 zajišťuje

a) jednoznačnou síťovou identifikaci zařízení původce, je-li v komunikační síti použit nástroj, který mění jeho síťovou identifikaci,
b) sběr informací o bezpečnostních a provozních událostech; zejména zaznamenává

1. datum a čas včetně specifikace časového pásma,
2. typ činnosti,

3. identifikaci technického aktiva, které činnost zaznamenalo,
4. jednoznačnou identifikaci účtu, pod kterým byla činnost provedena,
5. jednoznačnou síťovou identifikaci zařízení původce a
6. úspěšnost nebo neúspěšnost činnosti,

c) ochranu informací získaných podle písmen a) a b) před neoprávněným čtením a jakoukoli změnou,

d) zaznamenávání

1. přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů,
2. činností provedených administrátory,
3. úspěšné i neúspěšné manipulace s účty, oprávněními a právy,
4. neprovedení činností v důsledku nedostatku přístupových práv a oprávnění,
5. činností uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému,
6. zahájení a ukončení činností technických aktiv,
7. kritických i chybových hlášení technických aktiv a
8. přístupů k záznamům o událostech, pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí a

e) synchronizaci jednotného času technických aktiv nejméně jednou za 24 hodin.

(3) Povinná osoba uvedená v § 3 písm. c), d) a f) zákona uchovává záznamy událostí zaznamenaných podle odstavce 2 nejméně po dobu 18 měsíců.

(4) Povinná osoba uvedená v § 3 písm. e) zákona uchovává záznamy událostí zaznamenaných podle odstavce 2 nejméně po dobu 12 měsíců.

§ 23

Detekce kybernetických bezpečnostních událostí

(1) Povinná osoba v rámci komunikační sítě, jejíž součástí je informační a komunikační systém, používá nástroj pro detekci kybernetických bezpečnostních událostí, který zajistí

a) ověření a kontrolu přenášených dat v rámci komunikační sítě a mezi komunikačními sítěmi,

b) ověření a kontrolu přenášených dat na perimetru komunikační sítě a

c) blokování nežádoucí komunikace.

(2) Povinná osoba uvedená v § 3 písm. c), d) a f) zákona zajistí detekci kybernetických bezpečnostních událostí přiměřeně s ohledem na důležitost aktiv v rámci

a) koncových stanic,

b) mobilních zařízení,

c) serverů,

d) datových úložišť a výměnných datových nosičů,

e) síťových aktivních prvků a

f) obdobných aktiv.

§ 24

Sběr a vyhodnocování kybernetických bezpečnostních událostí

Povinná osoba uvedená v § 3 písm. c), d) a f) zákona používá nástroj pro sběr a nepřetržité vyhodnocení kybernetických bezpečnostních událostí, který umožní

a) sběr a vyhodnocování událostí zaznamenaných podle § 22 a 23,
b) vyhledávání a seskupování souvisejících záznamů,
c) poskytování informací pro určené bezpečnostní role o detekovaných kybernetických bezpečnostních událostech,
d) vyhodnocování kybernetických bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů, včetně včasného varování určených bezpečnostních rolí,
e) omezení případů nesprávného vyhodnocení událostí pravidelnou aktualizací nastavení pravidel pro
    1. vyhodnocování kybernetických bezpečnostních událostí a
    2. včasné varování a
f) využívání informací získaných nástrojem pro sběr a vyhodnocení kybernetických bezpečnostních událostí pro optimální nastavení bezpečnostních opatření informačního a komunikačního systému.

§ 25

Aplikační bezpečnost

(1) Povinná osoba provádí penetrační testy informačního a komunikačního systému se zaměřením na důležitá aktiva, a to
    a) před jejich uvedením do provozu a
    b) v souvislosti s významnou změnou podle § 11 odst. 3.

(2) Povinná osoba dále v rámci aplikační bezpečnosti zajistí trvalou ochranu aplikací, informací a transakcí před
    a) neoprávněnou činností a
    b) popřením provedených činností.

§ 26

Kryptografické prostředky

Povinná osoba pro ochranu aktiv informačního a komunikačního systému

a) používá aktuálně odolné kryptografické algoritmy a kryptografické klíče,
b) používá systém správy klíčů a certifikátů, který
    1. zajistí generování, distribuci, ukládání, změny, omezení platnosti, zneplatnění certifikátů a likvidaci klíčů a
    2. umožní kontrolu a audit,
c) prosazuje bezpečné nakládání s kryptografickými prostředky a

d) zohledňuje doporučení v oblasti kryptografických prostředků vydaná Úřadem, zveřejněná na jeho internetových stránkách.

§ 27

Zajišťování úrovně dostupnosti informací

Povinná osoba zavede opatření pro zajišťování úrovně dostupnosti, kterými zajistí

a) dostupnost informačního a komunikačního systému pro splnění cílů podle § 15,
b) odolnost informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům, které by mohly snížit jeho dostupnost,
c) dostupnost důležitých technických aktiv informačního a komunikačního systému a
d) redundanci aktiv nezbytných pro zajištění dostupnosti informačního a komunikačního systému.

§ 28

Průmyslové, řídicí a obdobné specifické systémy

Povinná osoba pro zajištění kybernetické bezpečnosti průmyslových, řídicích a obdobných specifických systémů používá nástroje a opatření, které zajistí

a) použití technických a programových prostředků, které jsou určeny do specifického prostředí,
b) omezení fyzického přístupu k zařízením těchto systémů a ke komunikační síti,
c) vyčlenění komunikační sítě určené pro tyto systémy od ostatní infrastruktury,
d) omezení a řízení vzdáleného přístupu k těmto systémům,
e) ochranu jednotlivých technických aktiv těchto systémů před využitím známých zranitelností a
f) obnovení chodu těchto systémů po kybernetickém bezpečnostním incidentu.

§ 29

Digitální služby

(1) Povinná osoba uvedená v § 3 písm. h) zákona zavede bezpečnostní opatření podle prováděcího nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148, pokud jde o bližší upřesnění prvků, které musí poskytovatelé digitálních služeb zohledňovat při řízení bezpečnostních rizik, jimiž jsou vystaveny sítě a informační systémy, a parametrů pro posuzování toho, zda je dopad incidentu významný; ustanovení § 3 až 28 se na tuto povinnou osobu nepoužijí.

(2) Povinná osoba uvedená v § 3 písm. h) zákona hlásí kontaktní údaje podle § 34 odst. 2.

(3) Povinná osoba uvedená v § 3 písm. h) zákona hlásí kybernetické bezpečnostní incidenty podle § 32 odst. 2 a 3.

HLAVA III
BEZPEČNOSTNÍ POLITIKA A BEZPEČNOSTNÍ DOKUMENTACE

§ 30

Bezpečnostní politika a bezpečnostní dokumentace

(1) Povinná osoba
   a) stanoví bezpečnostní politiku a vede bezpečnostní dokumentaci zahrnující oblasti uvedené v příloze č. 5,
   b) pravidelně přezkoumává bezpečnostní politiku a bezpečnostní dokumentaci a
   c) zajistí, aby byla bezpečnostní politika a bezpečnostní dokumentace aktuální.

(2) Bezpečnostní politika a bezpečnostní dokumentace musí být
   a) dostupné v listinné nebo elektronické podobě,
   b) komunikovány v rámci povinné osoby,
   c) přiměřeně dostupné dotčeným stranám,
   d) řízeny,
   e) chráněny z pohledu důvěrnosti, integrity a dostupnosti a
   f) vedeny tak, aby informace v nich obsažené byly úplné, čitelné, snadno identifikovatelné a snadno vyhledatelné.

ČÁST TŘETÍ
KYBERNETICKÝ BEZPEČNOSTNÍ INCIDENT

§ 31

Kategorizace kybernetických bezpečnostních incidentů

(1) Jednotlivé kybernetické bezpečnostní incidenty se kategorizují podle významnosti při zohlednění
   a) dopadů obsažených v dopadových určujících kritériích, podle kterých byly povinné osoby určeny,
   b) počtu dotčených uživatelů,
   c) způsobené nebo předpokládané škody,
   d) důležitosti dotčených aktiv informačního a komunikačního systému,
   e) dopadů na poskytované služby informačního a komunikačního systému,
   f) dopadů na služby poskytované jinými informačními a komunikačními systémy,
   g) délky trvání incidentu,
   h) zeměpisného rozsahu dotčené oblasti a
   i) dalších dopadů.

(2) Pro potřeby hlášení a zvládání kybernetických bezpečnostních incidentů se na základě zohlednění podle odstavce 1 kybernetické bezpečnostní incidenty zařadí do následujících kategorií

a) Kategorie III - velmi významný kybernetický bezpečnostní incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod,

b) Kategorie II - významný kybernetický bezpečnostní incident, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod, nebo

c) Kategorie I - méně významný kybernetický bezpečnostní incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod.

(3) Typy kybernetických bezpečnostních incidentů podle dopadu jsou

a) kybernetický bezpečnostní incident způsobující narušení důvěrnosti aktiv,

b) kybernetický bezpečnostní incident způsobující narušení integrity aktiv,

c) kybernetický bezpečnostní incident způsobující narušení dostupnosti aktiv, nebo

d) kybernetický bezpečnostní incident způsobující kombinaci dopadů uvedených v písmenech a) až c).

(4) Toto ustanovení se nevztahuje na kybernetické bezpečnostní incidenty u povinné osoby uvedené v § 3 písm. h) zákona.

§ 32

Forma a náležitosti hlášení kybernetických bezpečnostních incidentů

(1) Kybernetický bezpečnostní incident se Úřadu hlásí na elektronickém formuláři zveřejněném na internetových stránkách Úřadu zaslaném

a) na adresu elektronické pošty Úřadu určenou pro příjem hlášení kybernetických bezpečnostních incidentů, zveřejněnou na internetových stránkách Úřadu,

b) do datové schránky Úřadu, nebo

c) prostřednictvím datového rozhraní, pokud je používáno, jehož popis je zveřejněn na internetových stránkách Úřadu.

(2) Kybernetický bezpečnostní incident se provozovateli národního CERT hlásí na elektronickém formuláři zveřejněném na internetových stránkách provozovatele národního CERT zaslaném

a) na adresu elektronické pošty provozovatele národního CERT určenou pro příjem hlášení kybernetických bezpečnostních incidentů, zveřejněnou na jeho internetových stránkách,

b) do datové schránky provozovatele národního CERT, nebo

c) prostřednictvím internetových stránek provozovatele národního CERT.

(3) Hlášení kybernetického bezpečnostního incidentu je možné zaslat i v listinné podobě, avšak pouze v případech, kdy nelze využít žádný ze způsobů uvedených v odstavcích 1 a 2.

(4) Náležitosti hlášení kybernetického bezpečnostního incidentu jsou

a) identifikace odesilatele,

b) identifikace informačního a komunikačního systému,

c) datum a čas zjištění incidentu a

d) popis incidentu.

ČÁST ČTVRTÁ

REAKTIVNÍ OPATŘENÍ A KONTAKTNÍ ÚDAJE

§ 33

Reaktivní opatření

(1) Povinná osoba, které Úřad uložil provést reaktivní opatření,

a) posoudí očekávané dopady reaktivního opatření na informační a komunikační systém a na zavedená bezpečnostní opatření a vyhodnotí možné negativní účinky a

b) stanoví způsob rychlého provedení tohoto opatření, který minimalizuje jeho možné negativní účinky, a určí časový plán jeho provedení.

(2) Povinná osoba, které Úřad uložil provést reaktivní opatření, oznámí způsob provedení reaktivního opatření a jeho výsledek ve formě uvedené na internetových stránkách Úřadu.

§ 34

Kontaktní údaje

(1) Kontaktní údaje se Úřadu oznamují na elektronickém formuláři zveřejněném na internetových stránkách Úřadu zaslaném

a) na adresu elektronické pošty Úřadu určenou pro příjem oznámení kontaktních údajů, zveřejněnou na internetových stránkách Úřadu,

b) do datové schránky Úřadu, nebo

c) prostřednictvím datového rozhraní, pokud je používáno, jehož popis je zveřejněn na internetových stránkách Úřadu.

(2) Kontaktní údaje se provozovateli národního CERT oznamují na elektronickém formuláři zveřejněném na internetových stránkách provozovatele národního CERT zaslaném

a) na adresu elektronické pošty provozovatele národního CERT určenou pro příjem oznámení kontaktních údajů, zveřejněnou na jeho internetových stránkách,

b) do datové schránky provozovatele národního CERT, nebo

c) prostřednictvím internetových stránek provozovatele národního CERT.

(3) Hlášení kontaktních údajů je možné zaslat i v listinné podobě, avšak pouze v případech, kdy nelze využít žádný ze způsobů uvedených v odstavcích 1 a 2.

(4) Vzor oznámení kontaktních údajů je uveden v příloze č. 8 k této vyhlášce.

(5) Povinná osoba uvedená v § 3 písm. c) až f) zákona, která je provozovatelem, dále k hlášení kontaktních údajů podle odstavce 1 přikládá dokument, kterým ji správce prokazatelně informuje podle § 8 odst. 1 písm. c).

ČÁST PÁTÁ
ZÁVĚREČNÁ USTANOVENÍ

§ 35
Přechodná ustanovení

(1) V případě informačních systémů kritické informační infrastruktury a komunikačních systémů kritické informační infrastruktury, které byly určeny přede dnem nabytí účinnosti této vyhlášky, a v případě významných informačních systémů, u kterých došlo k naplnění určujících kritérií přede dnem nabytí účinnosti této vyhlášky, se do jednoho roku ode dne nabytí účinnosti této vyhlášky pro obsah a strukturu bezpečnostní dokumentace a obsah a rozsah zavedených bezpečnostních opatření použijí ustanovení vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti).

(2) V případě informačních systémů kritické informační infrastruktury a komunikačních systémů kritické informační infrastruktury, které byly určeny přede dnem nabytí účinnosti této vyhlášky, a v případě významných informačních systémů, u kterých došlo k naplnění určujících kritérií přede dnem nabytí účinnosti této vyhlášky, se do jednoho roku ode dne nabytí účinnosti této vyhlášky pro způsob likvidace dat, provozních údajů, informací a jejich kopií tato vyhláška nepoužije.

§ 36
Zrušovací ustanovení

Zrušuje se vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti).

§ 37
Účinnost

Tato vyhláška nabývá účinnosti dnem vyhlášení.

Ředitel:

Ing. Navrátil v. r.

Příloha č. 1 k vyhlášce č. 82/2018 Sb.

Hodnocení aktiv

(1) Pro hodnocení důležitosti aktiv jsou v tomto případě použity stupnice o čtyřech úrovních a posuzuje se, jaký dopad by mělo narušení bezpečnosti informací u jednotlivých aktiv. Povinná osoba může používat odlišný počet úrovní pro hodnocení důležitosti aktiv, než jaký je uveden v této příloze, dodrží-li jednoznačné vazby mezi jimi používaným způsobem hodnocení důležitosti aktiv a stupnicemi a úrovněmi pro hodnocení důležitosti aktiv, které jsou uvedeny v této příloze.

(2) Je doporučeno, aby si každá povinná osoba tyto dopadové matice přizpůsobila svým potřebám.

Tab. 1: Stupnice pro hodnocení důvěrnosti

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy povinné osoby. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle tzv. traffic light protokolu (dále jen „TLP“) je využíváno označení TLP:WHITE.	Není vyžadována žádná ochrana. Likvidace/mazání aktiva na úrovni Nízká – viz příloha č. 4.
Střední	Aktiva nejsou veřejně přístupná a tvoří know-how povinné osoby, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:GREEN nebo TLP:AMBER.	Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu. Likvidace/mazání aktiva na úrovni Střední – viz příloha č. 4.
Vysoká	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (například obchodní tajemství, osobní údaje). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:AMBER.	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací komunikační sítí jsou chráněny pomocí kryptografických prostředků. Likvidace/mazání aktiva na úrovni Vysoká – viz příloha č. 4.
Kritická	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:RED nebo TLP:AMBER.	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Dále metody ochrany zabraňující zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků.

		Likvidace/mazání aktiva na úrovni Kritická – viz příloha č. 4.

Tab. 2: Stupnice pro hodnocení integrity

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy povinné osoby.	Není vyžadována žádná ochrana.
Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby a může se projevit méně závažnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány standardní nástroje (například omezení přístupových práv pro zápis).
Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.
Kritická	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů povinné osoby s přímými a velmi vážnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (například pomocí technologie digitálního podpisu).

Tab. 3: Stupnice pro hodnocení dostupnosti

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).	Pro ochranu dostupnosti je postačující pravidelné zálohování.
Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů povinné osoby.	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.
Vysoká	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů povinné osoby.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být pod-

	něných zájmů povinné osoby. Aktiva jsou považována za velmi důležitá.	míněna zásahy obsluhy nebo výměnou technických aktiv.
Kritická	Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za kritická.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.

Příloha č. 2 k vyhlášce č. 82/2018 Sb.

Hodnocení rizik

(1) Jednoznačné stanovení funkce pro určení rizika je nezbytnou součástí metodiky pro hodnocení rizik podle § 5.

(2) Hodnota rizika je nejčastěji vyjádřena jako funkce, kterou ovlivňuje dopad, hrozba a zranitelnost.

(3) Pro hodnocení rizik lze použít například tuto funkci:

Riziko = dopad x hrozba x zranitelnost.

(4) Dopad je v tomto případě odvozen z hodnocení aktiv podle přílohy č. 1.

(5) V případě, že povinná osoba využívá metodu pro hodnocení rizik, která nerozlišuje hodnocení hrozby a zranitelnosti, je možné stupnice pro hodnocení hrozeb a zranitelností sloučit. Sloučení stupnic by nemělo vést ke ztrátě schopnosti rozlišení úrovně hrozby a zranitelnosti. Za tímto účelem lze použít například komentář, který zřetelně vyjádří jak úroveň hrozby, tak i úroveň zranitelnosti. Obdobně se postupuje i v případech, kdy povinná osoba používá jiný počet úrovní pro hodnocení dopadů, hrozeb, zranitelností a rizik.

Tab. 1: Stupnice pro hodnocení hrozeb

Úroveň	Popis
Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

Tab. 2: Stupnice pro hodnocení zranitelností

Úroveň	Popis

Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití.
Střední	Zneužití zranitelnosti je málo pravděpodobné až pravděpodobné. Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
Vysoká	Zneužití zranitelnosti je pravděpodobné až velmi pravděpodobné. Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
Kritická	Zneužití zranitelnosti je velmi pravděpodobné až víceméně jisté. Bezpečnostní opatření nejsou realizována nebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.

Tab. 3: Stupnice pro hodnocení rizik

Úroveň	Popis
Nízké	Riziko je považováno za akceptovatelné.
Střední	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko akceptovatelné.
Vysoké	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.
Kritické	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.

Příloha č. 3 k vyhlášce č. 82/2018 Sb.

Zranitelnosti a hrozby

Upozornění: Tato příloha obsahuje jen vybrané kategorie zranitelností a hrozeb. Identifikace konkrétních zranitelností a hrozeb je odpovědností povinné osoby.

Zranitelnosti

1. nedostatečná údržba informačního a komunikačního systému,
2. zastaralost informačního a komunikačního systému,

3. nedostatečná ochrana vnějšího perimetru,
4. nedostatečné bezpečnostní povědomí uživatelů a administrátorů,
5. nedostatečná údržba informačního a komunikačního systému,
6. nevhodné nastavení přístupových oprávnění,
7. nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
8. nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování,
9. nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí,
10. nedostatečná ochrana aktiv,
11. nevhodná bezpečnostní architektura,
12. nedostatečná míra nezávislé kontroly,
13. neschopnost včasného odhalení pochybení ze strany zaměstnanců.

Hrozby

1. porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů,
2. poškození nebo selhání technického anebo programového vybavení,
3. zneužití identity,
4. užívání programového vybavení v rozporu s licenčními podmínkami,
5. škodlivý kód (například viry, spyware, trojské koně),
6. narušení fyzické bezpečnosti,
7. přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie,
8. zneužití nebo neoprávněná modifikace údajů,
9. ztráta, odcizení nebo poškození aktiva,
10. nedodržení smluvního závazku ze strany dodavatele,
11. pochybení ze strany zaměstnanců,
12. zneužití vnitřních prostředků, sabotáž,
13. dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb,
14. nedostatek zaměstnanců s potřebnou odbornou úrovní,
15. cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik,
16. zneužití vyměnitelných technických nosičů dat,
17. napadení elektronické komunikace (odposlech, modifikace).

Příloha č. 4 k vyhlášce č. 82/2018 Sb.

Likvidace dat

(1) Tato příloha udává povinnosti správce informačního a komunikačního systému k definování způsobů mazání dat a způsobů likvidace technických nosičů informace, provozních údajů, informací a jejich kopií.

(2) Jednotliví správci informačního a komunikačního systému si stanoví pravidla pro mazání dat a likvidaci technických nosičů dat v souladu s touto přílohou. Tím nejsou dotčeny povinnosti

podle jiných právních předpisů. Je nutné zvolit adekvátní úroveň služby nabízející přiměřená bezpečnostní opatření, včetně adekvátních pravidel pro mazání dat a likvidaci technických nosičů dat, vzhledem k hodnotě a důležitosti aktiv.

(3) Pravidla pro likvidaci dat by měla být stanovena přiměřeně hodnotě a důležitosti aktiv a měla by zejména zohledňovat

a) hodnotu aktiva (zejména z pohledu důvěrnosti),
b) technologii (typy a velikost nosičů informace),
c) zda se nosič informace nachází pod kontrolou organizace či nikoliv,
d) zda jsou data součástí dedikovaného nebo multitenantního prostředí,
e) kdo bude likvidaci dat provádět (interní zaměstnanec, nebo dodavatel),
f) dostupnost vybavení a nástrojů pro likvidaci,
g) kapacitu likvidovaných nosičů,
h) zda je k dispozici vyškolený personál,
i) časovou náročnost likvidace,
j) cenu likvidace s ohledem na nástroje, školení, validaci, opětovné využití nosiče informace
k) možné způsoby likvidace dat (například zničením nosiče, několikanásobným přepsáním nosiče dat, znečitelněním dat jejich šifrováním a podobně),
l) použitelné způsoby likvidace dat vzhledem ke stavu nosiče informace (například při poškození zařízení nebude možné použít variantu přepisu informace, ale některý ze způsobů fyzické likvidace).

(4) Způsoby likvidace technických nosičů informace, provozních údajů, informací a jejich kopií:

a) Odstranění

1. Způsob likvidace spočívá v odstranění dat tak, aby byla pro systém nedostupná (například odstranění datového souboru, vyhození tištěného dokumentu do odpadu).
2. Jde o nejméně bezpečný způsob likvidace dat. V případě získání nosiče informace je možné s vynaložením určitého úsilí informace obnovit.
3. Tato metoda není použitelná pro nosiče digitálních dat neumožňující opětovný zápis.
4. Použitelný způsob pro úroveň důvěrnosti aktiva (vychází z přílohy č. 1): nízká.

b) Přepsání

1. Způsob likvidace spočívá v přepsání chráněné informace nahodilými hodnotami.
2. Jde o středně bezpečný způsob likvidace dat. Volně dostupné nástroje neumožňují obnovení přepsaných informací.
3. Přepsání může být nahrazeno nebo kombinováno bezpečnou likvidací kryptografických klíčů k zašifrované informaci.
4. Tato metoda není vhodná pro poškozená média, média neumožňující opětovný zápis, případně pro média s velkou kapacitou.
5. Použitelný způsob pro úroveň důvěrnosti aktiva (vychází z přílohy č. 1): nízká až kritická.

c) Fyzická likvidace nosiče informace

1. Způsob likvidace spočívající ve zničení nosiče informace, popřípadě v rozebrání zařízení a následném zničení nosiče informace (mechanickým, chemickým či tepelným působením).
2. Jde o nejbezpečnější metodu likvidace dat. Nosič informace po fyzické likvidaci nelze znovu použít pro původní účel. Původní informace není možné obnovit ani při vynaložení velkého množství prostředků a úsilí.
3. Použitelný způsob likvidace pro úroveň důvěrnosti aktiva (vychází z přílohy č. 1): střední až kritická.

Příklad možných způsobů likvidace podle úrovně důvěrnosti aktiva (vychází z přílohy č. 1)

<table>
<tr><td></td><td colspan="4">Přípustný způsob likvidace podle úrovně důležitosti aktiva</td></tr>
<tr><td>Nosič informace</td><td>1. Nízká</td><td>2. Střední</td><td>3. Vysoká</td><td>4. Kritická</td></tr>
<tr><td>Informace na lidsky čitelném nosiči (tištěné dokumenty, poznámky a podobně)</td><td>Odstranění: Vyhození do odpadu.</td><td>Přepsání: Začernění.

Fyzická likvidace: Znehodnocení nosiče informací použitím skartovacího stroje.</td><td colspan="2">Fyzická likvidace: Znehodnocení nosiče informací použitím skartovacího stroje s podélným i příčným řezem, spálením nebo rozložením.</td></tr>
<tr><td>Mobilní zařízení (mobilní telefony, tablety)</td><td>Odstranění: Vymazání informací, reset zařízení do továrního nastavení.</td><td>Přepsání: Pro zařízení s šifrovaným úložištěm – odstranění informací a reset do továrního nastavení.</td><td colspan="2" rowspan="3">Fyzická likvidace: Rozebrání zařízení a zničení nosiče informací.</td></tr>
<tr><td>Síťová zařízení (router, switch, modem a podobně)

Kancelářské vybavení (scanery, tiskárny, fax)</td><td>Odstranění: Vymazání informací, reset do továrního nastavení.</td><td>Přepsání: Odstranění a zahlcení umělými událostmi (umělý síťový provoz, testovací tiskové úlohy a podobně.).</td></tr>
<tr><td>Magnetická média (magnetické pá-</td><td>Odstranění: Smazání dat na úrovni</td><td>Přepsání: Přepsání dat. V případě šifrova-</td></tr>
</table>

<table>
<tr><td>sky, disky, HDD [Hard Disk Drive])</td><td rowspan="3">souborového systému.</td><td rowspan="2">ného média je alternativou bezpečná likvidace kryptografických klíčů</td><td></td><td></td></tr>
<tr><td>Optická média (CD, DVD, HD-DVD, BLU-RAY)</td><td colspan="2" rowspan="2">Fyzická likvidace:
Zničení nosiče informací.</td></tr>
<tr><td>Elektronická média (flash paměti)</td><td>Fyzická likvidace.</td></tr>
<tr><td rowspan="2">Outsourcing a cloud</td><td colspan="4">Přípustný způsob likvidace dat by měl být stanoven smluvním ujednáním.</td></tr>
<tr><td>Odstranění:
Odstranění všech souborů včetně předchozích verzí.</td><td>Přepsání:
Použití šifrování datových úložišť na úrovni paměťového média a bezpečná likvidace kryptografických klíčů.

Alternativně v případě dedikovaného paměťového média je možné data po ukončení služby přepsat.</td><td>Přepsání:
Použití šifrování datových úložišť na úrovni paměťového média a bezpečná likvidace kryptografických klíčů uložených v certifikovaném hardware security modulu (HSM) řízená zákazníkem (například podle standardu FIPS 140-2 Level 2). Při ukončení služby bude zlikvidován vrchní přístupový klíč a data jsou přepsána.</td><td>Přepsání/fyzická likvidace: Použit způsob viz úroveň “3. Vysoká” nebo použita dedikovaná paměťová kapacita úložiště. Při ukončení služby provedena celková sanitizace všech použitých paměťových médií podle výše uvedených řádků pro úroveň kritická.</td></tr>
</table>

Příloha č. 5 k vyhlášce č. 82/2018 Sb.

Obsah bezpečnostní politiky a bezpečnostní dokumentace

1. Bezpečnostní politika

1.1. Politika systému řízení bezpečnosti informací

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.

1.2. Politika řízení aktiv

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 mazání nebo ničení technických nosičů dat, informací, provozních údajů a jejich kopií.

1.3. Politika organizační bezpečnosti

a) Určení bezpečnostních rolí a jejich práv a povinností.
b) Požadavky na oddělení výkonu činností jednotlivých bezpečnostních rolí.
c) Požadavky na oddělení výkonu bezpečnostních a provozních rolí.

1.4. Politika řízení dodavatelů

a) Pravidla a principy pro výběr dodavatelů.
b) Pravidla pro hodnocení rizik souvisejících s dodavateli.
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.

1.5. Politika bezpečnosti lidských zdrojů

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 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.

1.6 Politika řízení provozu a komunikací

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

1.7. Politika řízení přístupu

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.

1.8. Politika bezpečného chování uživatelů

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.

1.9. Politika zálohování a obnovy a dlouhodobého ukládání

a) Požadavky na zálohování a obnovu.
b) Pravidla a postupy zálohování.
c) Pravidla a postupy dlouhodobého ukládání.
d) Pravidla bezpečného zálohování a dlouhodobého ukládání informací.
e) Pravidla a postupy obnovy.
f) Pravidla a postupy testování zálohování a obnovy.
g) Politika přístupu k zálohám, ukládaným informacím.

1.10. Politika bezpečného předávání a výměny informací

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

1.11. Politika řízení technických zranitelností

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.

1.12. Politika bezpečného používání mobilních zařízení

a) Pravidla a postupy pro bezpečné používání mobilních zařízení.
b) Pravidla a postupy pro zajištění bezpečnosti zařízení, která povinná osoba nemá ve své správě.

1.13. Politika akvizice, vývoje a údržby

a) Bezpečnostní požadavky pro akvizici, vývoj a údržbu.
b) Řízení zranitelností.
c) Politika poskytování a nabývání licencí programového vybavení a informací

1. pravidla a postupy nasazení programového vybavení a jeho evidence,
2. pravidla a postupy pro kontrolu dodržování licenčních podmínek.

1.14. Politika ochrany osobních údajů

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.

1.15. Politika fyzické bezpečnosti

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

1.16. Politika bezpečnosti komunikační sítě

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.

1.17. Politika ochrany před škodlivým kódem

a) Pravidla a postupy pro ochranu síťové komunikace.
b) Pravidla a postupy pro ochranu serverů a sdílených datových úložišť.
c) Pravidla a postupy pro ochranu pracovních stanic.

1.18. Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí

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.

1.19. Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí

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.

1.20. Politika bezpečného používání kryptografické ochrany

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.

1.21. Politika řízení změn

a) Způsob a principy řízení významných změn v rámci povinné osoby, jejich procesech, informačních a komunikačních systémech.
b) Přezkoumávání dopadů významných změn.
c) Způsob vedení evidence a testování významných změn.

1.22. Politika zvládání kybernetických bezpečnostních incidentů

a) Definování kategorií kybernetického bezpečnostního incidentu.
b) Pravidla a postupy pro identifikaci, 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.
e) Evidence incidentů.

1.23. Politika řízení kontinuity činností

a) Práva a povinnosti zúčastněných osob.
b) Cíle řízení kontinuity činností

1. minimální úroveň poskytovaných služeb,
2. doba obnovení chodu,
3. bod obnovení dat.

c) Politika 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 a havarijních plánů.

f) Postupy pro realizaci opatření vydaných Úřadem.

2. Obsah bezpečnostní dokumentace

2.1. Zpráva z auditu kybernetické bezpečnosti

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.

2.2. 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 systému řízení bezpečnosti informací.

d) Výsledky hodnocení rizik a stav plánu zvládání rizik.
e) Identifikace možností pro neustálé zlepšování.
f) Doporučení potřebných rozhodnutí, stanovení opatření a osob zajišťujících výkon jednotlivých činností.

2.3. Metodika pro identifikaci a hodnocení aktiv a pro hodnocení rizik

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 akceptovatelných rizik.

2.4. Zpráva o hodnocení aktiv a rizik

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

1. identifikace a popis podpůrných aktiv,
2. určení garantů podpůrných aktiv,
3. určení vazeb mezi primárními a podpůrnými aktivy.

c) 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 akceptovatelnost rizik,
5. určení a schválení akceptovatelných rizik.

d) Zvládání rizik

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

2.5. Prohlášení o aplikovatelnosti

a) Přehled vyloučených bezpečnostních opatření požadovaných touto vyhláškou včetně zdůvodnění, proč nebyla aplikována.
b) Přehled zavedených bezpečnostních opatření včetně způsobu jejich implementace.

2.6. Plán zvládání rizik

a) Obsah a cíle vybraných bezpečnostních opatření pro zvládání rizik včetně vazby na konkrétní rizika.
b) Potřebné zdroje pro jednotlivá bezpečnostní opatření pro zvládání rizik.
c) Osoby zajišťující jednotlivá bezpečnostní opatření pro zvládání rizik.
d) Termíny zavedení jednotlivých bezpečnostních opatření pro zvládání rizik.
e) Způsob realizace bezpečnostních opatření.
f) Způsoby hodnocení úspěšnosti zavedení jednotlivých bezpečnostních opatření pro zvládání rizik.

2.7. Plán rozvoje bezpečnostního povědomí

a) Obsah a termíny poučení uživatelů, administrátorů a osob zastávajících bezpečnostní role.
b) Obsah a termíny poučení nových zaměstnanců.
c) Přehledy, které obsahují předmět jednotlivých školení a seznam osob, které školení absolvovaly.
d) Formy a způsoby hodnocení plánu.

2.8. Evidence změn

a) Evidence životního cyklu významných změn.
b) Záznamy o změnách konfigurace podpůrných aktiv.

2.9. Hlášené kontaktní údaje

Přehled hlášených kontaktních údajů.

2.10. 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.

2.11. Další doporučená dokumentace

a) Topologie infrastruktury.
b) Přehled síťových zařízení.

Příloha č. 6 k vyhlášce č. 82/2018 Sb.

Výbor pro řízení kybernetické bezpečnosti a bezpečnostní role

Tato příloha obsahuje popis doporučených požadavků pro výbor pro řízení kybernetické bezpečnosti a bezpečnostní role uvedené v § 6 a 7.

Tab. 1: Výbor pro řízení kybernetické bezpečnosti

Role:	**Výbor pro řízení kybernetické bezpečnosti**
Klíčové činnosti:	a) Odpovědnost za 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.
Další podmínky:	a) Člen výboru pro řízení kybernetické bezpečnosti musí být alespoň 1. zástupce vrcholového vedení nebo jím pověřené osoby, 2. manažer kybernetické bezpečnosti. b) Členové výboru pro řízení kybernetické bezpečnosti se pravidelně scházejí, přičemž průběh a výstupy z jednání jsou uchovávány v listinné nebo elektronické podobě.

Tab. 2: Manažer kybernetické bezpečnosti

Role:	Manažer kybernetické bezpečnosti
Klíčové činnosti:	a) Odpovědnost za řízení systému řízení bezpečnosti informací. b) Pravidelný reporting pro vrcholové vedení povinné osoby. c) Pravidelná komunikace s vrcholovým vedením povinné osoby. d) Předkládání Zpráv o hodnocení aktiv a rizik, Plánu zvládání rizik a Prohlášení o aplikovatelnosti výboru pro řízení kybernetické bezpečnosti. e) Poskytování pokynů pro zajištění bezpečnosti informací při vytváření, hodnocení, výběru, řízení a ukončení dodavatelských vztahů v oblasti ICT. f) Komunikace s GovCERT/CSIRT. g) Podílení se na procesu řízení rizik. 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 zákon. 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.
Vzdělání a praxe:	a) Alespoň 3 roky praxe v oboru informační nebo kybernetické bezpečnosti, nebo b) absolvování studia na vysoké škole a alespoň 1 rok praxe v oboru informační nebo kybernetické bezpečnosti.
Relevantní certifikace*:	Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Security Professional (CISSP), Manažer BI (akreditační schéma ČIA).
Další podmínky:	a) Role není slučitelná s rolemi odpovědnými za provoz informačního a komunikačního systému a s dalšími provozními či řídicími rolemi. b) Pro správný výkon této role je zapotřebí zajistit potřebné pravomoci, odpovědnost a rozpočet.

Tab. 3: Architekt kybernetické bezpečnosti

Role:	Architekt kybernetické bezpečnosti
Klíčové činnosti:	a) Odpovědnost za návrh implementace bezpečnostních opatření. b) Zajišťování architektury bezpečnosti.

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 architektury bezpečnosti se zaměřením na cíle a bezpečnost. c) Bezpečnost vývoje softwaru.
Vzdělání a praxe:	a) Alespoň 3 roky praxe v oboru informační nebo kybernetické bezpečnosti, nebo b) absolvování studia na vysoké škole a alespoň 1 rok praxe v oboru informační nebo kybernetické bezpečnosti.
Relevantní certifikace*:	Certified Ethical Hacker (CEH), CompTIA Security +, Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Security Professional (CISSP), Manažer BI (akreditační schéma ČIA).
Další podmínky:	Role není slučitelná s rolemi odpovědnými za provoz informačních a komunikačních systémů.

Tab. 4: Auditor kybernetické bezpečnosti

Role:	**Auditor kybernetické bezpečnosti**
Klíčové činnosti:	Provádění auditu kybernetické bezpečnosti.
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.
Vzdělání a praxe:	a) Alespoň 3 roky praxe v oblasti auditu informační nebo kybernetické bezpečnosti, nebo b) absolvování studia na vysoké škole a alespoň 1 rok praxe v oblasti auditu informační nebo kybernetické bezpečnosti.
Relevantní certifikace*:	Certified Information Systems Auditor (CISA), Certified Internal Auditor (CIA), Certified in Risk and Information Systems Control (CRISC), Lead Auditor Information Security Management System (Lead Auditor ISMS), Auditor BI (akreditační schéma ČIA).
Další podmínky:	a) Role není slučitelná s rolemi 1. výboru pro řízení kybernetické bezpečnosti, 2. manažera kybernetické bezpečnosti, 3. architekta kybernetické bezpečnosti, 4. garanta aktiva. b) Role není slučitelná s rolemi odpovědnými za provoz informačních a komunikačních systémů.

Tab. 5: Garant aktiva

Role:	**Garant aktiva**
Klíčové činnosti:	a) Odpovědnost za zajištění rozvoje, použití a bezpečnosti aktiva. b) Spolupráce s ostatními osobami zastávajícími bezpečnostní role.
Znalosti:	a) Dobrá znalost aktiva, jehož je garantem. b) Dobrá znalost interních bezpečnostních politik a metodik (například Metodika pro hodnocení aktiv a rizik).

* Certifikace může být i jiná než uvedená, jestliže certifikace dokládající odbornou způsobilost bezpečnostních rolí splňuje požadavky ISO 17 024.

Příloha č. 7 k vyhlášce č. 82/2018 Sb.

Řízení dodavatelů - bezpečnostní opatření pro smluvní vztahy

Obsah smlouvy uzavírané s významnými dodavateli:

a) ustanovení o bezpečnosti informací (z pohledu důvěrnosti, dostupnosti a integrity),

b) ustanovení o oprávnění užívat data,

c) ustanovení o autorství programového kódu, popřípadě o programových licencích,

d) ustanovení o kontrole a auditu dodavatele (pravidla zákaznického auditu),

e) ustanovení upravující řetězení dodavatelů, přičemž musí být zajištěno, že poddodavatelé se zaváží dodržovat v plném rozsahu ujednání mezi povinnou osobou a dodavatelem a nebudou v rozporu s požadavky povinné osoby na dodavatele,

f) ustanovení o povinnosti dodavatele dodržovat bezpečnostní politiky povinné osoby nebo ustanovení o odsouhlasení bezpečnostních politik dodavatele povinnou osobou,

g) ustanovení o řízení změn,

h) ustanovení o souladu smluv s obecně závaznými právními předpisy,

i) ustanovení o povinnosti dodavatele informovat povinnou osobu o

   1. kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy,
   2. způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním smlouvy,
   3. významné změně ovládání tohoto dodavatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných tímto dodavatelem k plnění podle smlouvy se správcem,

j) specifikace podmínek z pohledu bezpečnosti při ukončení smlouvy (například přechodné období při ukončení spolupráce, kdy je třeba ještě udržovat službu před nasazením nového řešení, migrace dat a podobně),

k) specifikace podmínek pro řízení kontinuity činností v souvislosti s dodavateli (například zahrnutí dodavatelů do havarijních plánů, úkoly dodavatelů při aktivaci řízení kontinuity činností),

l) specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání správcem,

m) pravidla pro likvidaci dat,

n) ustanovení o právu jednostranně odstoupit od smlouvy v případě významné změny kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými dodavatelem k plnění podle smlouvy a

o) ustanovení o sankcích za porušení povinností.

Příloha č. 8 k vyhlášce č. 82/2018 Sb.

Vzor Formuláře pro hlášení kontaktních údajů

Vzor Formuláře pro hlášení kontaktních údajů

Národní centrum kybernetické bezpečnosti

Národní úřad pro kybernetickou a informační bezpečnost

ZKB - Formulář pro hlášení kontaktních údajů			
Datum:		Typ hlášení:	*prvotní hlášení* *hlášení změn*
A: Údaje o orgánu a osobě uvedené v § 3 zákona			
Název fyzické nebo právnické osoby *:			
Typ orgánu a osoby *:	*Provozovatel KII/PZS/VIS*		
	Poskytovatel digitálních služeb		
	Správce KII/PZS/VIS		
Adresa sídla *:			
Identifikační číslo orgánu nebo osoby (IČ) *:			
****K hlášení přiložte kopii dokumentu, kterým jste byli ze strany správce systému informováni o tom, že se stáváte provozovatelem dle § 3 zákona č. 181/2014 Sb.**			
B: Identifikace informačního nebo komunikačního systému			
Název správce systému**:			
Název systému*:			
Typ systému*:	*Kritická informační infrastruktura (KII)*		
	Informační systém základní služby		
	Významný informační systém (VIS)		
Informace týkající se zajišťovaných služeb a prostředků:			
Je systém dostupný prostřednictvím internetu?		*ano*	*ne*
Rozsah veřejných IP adres:			
Používaná doménová jména:			

Typ provozované činnosti:**

☐ správa/provoz
☐ vývoj
☐ systémový integrátor
☐ bezpečnostní dohled
☐ ostatní

C: Údaje o fyzické osobě, která je orgánem nebo osobou uvedenou v § 3 zákona oprávněna jednat ve věcech upravených zákonem

jméno, příjmení, vč. titulu*:	telefon - pevná linka*:	mobilní telefon*:	e-mail*:	role:

D: Významné sítě***

Subjekt zajišťující síť elektronických komunikací pro KII:

UPOZORNĚNÍ:

Aktuální verze vzoru Formuláře pro hlášení kontaktních údajů naleznete na internetových stránkách Úřadu.

Vyplněný formulář prosím uložte do PDF a odešlete jej do datové schránky NÚKIB, příp. opatřený elektronickým podpisem jej zašlete na e-mail nckb@nukib.cz. NEPOSÍLEJTE PROSÍM NASKENOVANÉ DOKUMENTY.

nehodící přeškrtnout
* Povinná pole
** Týká se pouze provozovatele
*** Vyplní pouze KII

[1]) Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.