Ministerstvo zdravotnictví České republiky Palackého nám. č 4, 128 01 Praha 2, IČ: 00024341	
	**Verze: v1/01** Platnost nové verze od: Spisový znak: Skartační znak a lhůta: V/5

Srovnání znění vyhlášky o kybernetické bezpečnosti

Implementace zákona č. 181/2014 Sb., o kybernetické bezpečnosti

Pořadí revize	Provedené dne	Zpracoval	Schválil
0.	17. 7. 2018	**Tomáš Bezouška,** Architekt kybernetické bezpečnosti MZČR	**Jiří Borej,** Manažer kybernetické bezpečnosti MZČR
1.			

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
316 VYHLÁŠKA ze dne 15. prosince 2014 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) Národní bezpečnostní úřad stanoví podle § 28 odst. 2 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), (dále jen „zákon“) k provedení § 6 písm. a) až c), § 8 odst. 4, § 13 odst. 4 a § 16 odst. 6 zákona.	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** Touto vyhláškou se stanoví obsah a struktura bezpečnostní dokumentace pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém, obsah bezpečnostních opatření, rozsah jejich zavedení, typy a kategorie kybernetických bezpečnostních incidentů, náležitosti a způsob hlášení kybernetického bezpečnostního incidentu, náležitosti oznámení o provedení reaktivního opatření a jeho výsledku a vzor oznámení kontaktních údajů a jeho formu.	**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,

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
	f) vzor oznámení kontaktních údajů a jeho formu a **g)** způsob likvidace dat, provozních údajů, informací a jejich kopií.
§ 2 **Vymezení pojmů** V této vyhlášce se rozumí **a)** systémem řízení bezpečnosti informací část systému řízení orgánu a osoby uvedené v § 3 písm. c) až e) zákona 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, **b)** aktivem primární aktivum a podpůrné aktivum, **c)** primárním aktivem informace nebo služba, kterou zpracovává nebo poskytuje informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém, **d)** podpůrným aktivem 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, **e)** technickým aktivem 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, **f)** rizikem možnost, že určitá hrozba využije zranitelnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému a způsobí poškození	§ 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,

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
aktiva, **g)** hodnocením rizik proces, při němž je určována významnost rizik a jejich přijatelná úroveň, **h)** řízením rizik činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik, **i)** hrozbou potencionální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, jejímž výsledkem může být poškození aktiva, **j)** zranitelností slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami, **k)** přijatelným rizikem riziko zbývající po uplatnění bezpečnostních opatření, jehož úroveň odpovídá kritériím pro přijatelnost rizik, **l)** bezpečnostní politikou soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv orgánem a osobou uvedenou v § 3 písm. c) až e) zákona, **m)** garantem aktiva fyzická osoba pověřená orgánem nebo osobou uvedenou v § 3 písm. c) až e) zákona k zajištění rozvoje, použití a bezpečnosti aktiva, **n)** uživatelem fyzická nebo právnická osoba anebo orgán veřejné moci, která využívá primární aktiva, **o)** administrátorem fyzická osoba pověřená garantem aktiva zajišťující správu, provoz, použití, údržbu a bezpečnost technického aktiva.	**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.

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
ČÁST DRUHÁ **BEZPEČNOSTNÍ OPATŘENÍ** **HLAVA I** **ORGANIZAČNÍ OPATŘENÍ** **§ 3** **Systém řízení bezpečnosti informací** **(1)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona v rámci systému řízení bezpečnosti informací **a)** stanoví s ohledem na aktiva a organizační bezpečnost rozsah a hranice systému řízení bezpečnosti informací, ve kterém určí, kterých organizačních částí a technických prvků se systém řízení bezpečnosti informací týká, **b)** řídí rizika podle § 4 odst. 1, **c)** 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 § 5 a zavede příslušná bezpečnostní opatření, **d)** monitoruje účinnost bezpečnostních opatření, **e)** vyhodnocuje vhodnost a účinnost bezpečnostní politiky podle § 5, **f)** zajistí provedení auditu kybernetické bezpečnosti podle § 15, a to nejméně jednou ročně, **g)** zajistí vyhodnocení účinnosti systému řízení bezpečnosti informací, které obsahuje hodnocení stavu systému řízení bezpečnosti informací včetně revize hodnocení rizik, posouzení výsledků provedených kontrol a auditů kybernetické bezpečnosti a dopadů kybernetických bezpečnostních incidentů na systém řízení bezpečnosti informací, a to nejméně jednou ročně, **h)** aktualizuje systém řízení bezpečnosti informací a příslušnou dokumentaci na	**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

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
základě zjištění auditů kybernetické bezpečnosti, výsledků vyhodnocení účinnosti systému řízení bezpečnosti informací a v souvislosti s prováděnými nebo plánovanými změnami a **i)** řídí provoz a zdroje systému řízení bezpečnosti informací, zaznamenává činnosti spojené se systémem řízení bezpečnosti informací a řízením rizik. **(2)** Orgán a osoba uvedená v § 3 písm. e) zákona v rámci systému řízení bezpečnosti informací **a)** řídí rizika podle § 4 odst. 2, **b)** 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 § 5, a zavede příslušná bezpečnostní opatření a **c)** provádí aktualizaci 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.	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.
§ 8 **Řízení aktiv** **(1)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona v rámci řízení aktiv **a)** identifikuje a eviduje primární aktiva, **b)** určí garanty aktiv, kteří jsou odpovědní za primární aktiva, a **c)** hodnotí důležitost primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti a zařadí je do jednotlivých úrovní minimálně v rozsahu podle přílohy č. 1 k této vyhlášce. **(2)** Při hodnocení důležitosti primárních aktiv je třeba především posoudit **a)** rozsah a důležitost osobních údajů nebo obchodního tajemství, **b)** rozsah dotčených právních povinností nebo jiných závazků,	**§ 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

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
c) rozsah narušení vnitřních řídících a kontrolních činností, **d)** poškození veřejných, obchodních nebo ekonomických zájmů, **e)** možné finanční ztráty, **f)** rozsah narušení běžných činností orgánu a osoby uvedené v § 3 písm. c) až e) zákona, **g)** dopady spojené s narušením důvěrnosti, integrity a dostupnosti a **h)** dopady na zachování dobrého jména nebo ochranu dobré pověsti. **(3)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále **a)** identifikuje a eviduje podpůrná aktiva, **b)** určí garanty aktiv, kteří jsou odpovědní za podpůrná aktiva, a **c)** určí vazby mezi primárními a podpůrnými aktivy a hodnotí důsledky závislostí mezi primárními a podpůrnými aktivy. **(4)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona dále **a)** stanoví pravidla ochrany, nutná pro zabezpečení jednotlivých úrovní aktiv tím, že **1.** určí způsoby rozlišování jednotlivých úrovní aktiv, **2.** stanoví pravidla pro manipulaci a evidenci s aktivy podle úrovní aktiv, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv a **3.** stanoví přípustné způsoby používání aktiv, **b)** zavede pravidla ochrany odpovídající úrovni aktiv a **c)** určí způsoby pro spolehlivé smazání nebo ničení technických nosičů dat s ohledem na úroveň aktiv.	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.

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
§ 4 **Řízení rizik** **(1)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona v rámci řízení rizik **a)** stanoví metodiku pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik včetně stanovení kritérií pro přijatelnost rizik, **b)** identifikuje a hodnotí důležitost aktiv, která patří do rozsahu systému řízení bezpečnosti informací, podle § 8 v rozsahu přílohy č. 1 k této vyhlášce a výstupy zapracuje do zprávy o hodnocení aktiv a rizik, **c)** identifikuje rizika, při kterých zohlední hrozby a zranitelnosti, posoudí možné dopady na aktiva, hodnotí tato rizika minimálně v rozsahu podle přílohy č. 2 k této vyhlášce, určí a schválí přijatelná rizika a zpracuje zprávu o hodnocení aktiv a rizik, **d)** zpracuje na základě bezpečnostních potřeb a výsledků hodnocení rizik prohlášení o aplikovatelnosti, které obsahuje přehled vybraných a zavedených bezpečnostních opatření, **e)** zpracuje a zavede plán zvládání rizik, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání rizik, určení osoby zajišťující 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 a **f)** zohlední bez zbytečného odkladu reaktivní a ochranná opatření vydaná Národním bezpečnostním úřadem (dále jen „Úřad“) 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, doplní plán zvládání rizik. **(2)** Orgán a osoba uvedená v § 3 písm. e) zákona v rámci řízení rizik **a)** stanoví metodiku pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik včetně stanovení kritérií pro přijatelnost rizik, **b)** identifikuje a hodnotí důležitost primárních aktiv, která patří do rozsahu 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,

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
řízení bezpečnosti informací, podle § 8 minimálně v rozsahu přílohy č. 1 k této vyhlášce a výstupy zapracuje do zprávy o hodnocení aktiv a rizik, **c)** identifikuje rizika, při kterých zohlední hrozby a zranitelnosti, posoudí možné dopady na primární aktiva, hodnotí tato rizika minimálně v rozsahu podle přílohy č. 2 k této vyhlášce a zpracuje zprávu o hodnocení aktiv a rizik, **d)** zpracuje na základě bezpečnostních potřeb a výsledků hodnocení rizik prohlášení o aplikovatelnosti, které obsahuje přehled vybraných a zavedených bezpečnostních opatření, **e)** zpracuje a zavede plán zvládání rizik, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání rizik, určení osoby zajišťující prosazování bezpečnostních opatření pro zvládání rizik, potřebné finanční, technické, lidské a informační zdroje, termíny jejich zavedení a popis vazeb mezi identifikovanými riziky a příslušnými bezpečnostními opatřeními a **f)** zohlední bez zbytečného odkladu reaktivní a ochranná opatření vydaná Úřadem 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, doplní plán zvládání rizik. **(3)** Řízení rizik může být zajištěno i jinými způsoby, než jak je stanoveno v odstavcích 1 a 2, pokud orgán a osoba uvedená v § 3 písm. c) až e) zákona zabezpečí, že používá opatření zajišťující stejnou nebo vyšší úroveň řízení rizik. **(4)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona při hodnocení rizik zvažuje zejména tyto hrozby **a)** porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů, **b)** poškození nebo selhání technického anebo programového vybavení, **c)** zneužití identity fyzické osoby, **d)** užívání programového vybavení v rozporu s licenčními podmínkami, **e)** kybernetický útok z komunikační sítě,	**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.

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
f) škodlivý kód (například viry, spyware, trojské koně), **g)** nedostatky při poskytování služeb informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému, **h)** narušení fyzické bezpečnosti, **i)** přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie, **j)** zneužití nebo neoprávněná modifikace údajů, **k)** trvale působící hrozby a **l)** odcizení nebo poškození aktiva. **(5)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona při hodnocení rizik zvažuje zejména tyto zranitelnosti **a)** nedostatečná ochrana vnějšího perimetru, **b)** nedostatečné bezpečnostní povědomí uživatelů a administrátorů, **c)** nedostatečná údržba informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému, **d)** nevhodné nastavení přístupových oprávnění, **e)** nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů, **f)** nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování a **g)** nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí. **(6)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona při hodnocení rizik dále	

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
zvažuje tyto hrozby **a)** porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany administrátorů kritické informační infrastruktury, **b)** pochybení ze strany zaměstnanců, **c)** zneužití vnitřních prostředků, sabotáž, **d)** dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb, **e)** nedostatek zaměstnanců s potřebnou odbornou úrovní, **f)** cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik a **g)** zneužití vyměnitelných technických nosičů dat. **(7)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona při hodnocení rizik dále zvažuje tyto zranitelnosti **a)** nedostatečná ochrana prostředků kritické informační infrastruktury, **b)** nevhodná bezpečnostní architektura, **c)** nedostatečná míra nezávislé kontroly a **d)** neschopnost včasného odhalení pochybení ze strany zaměstnanců.	
§ 6 **Organizační bezpečnost** **(1)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona zavede organizaci řízení bezpečnosti informací, v rámci které určí 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. **(2)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona určí bezpečnostní role **a)** manažer kybernetické bezpečnosti,	**§ 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,

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
b) architekt kybernetické bezpečnosti, **c)** auditor kybernetické bezpečnosti a **d)** garant aktiva podle § 2 písm. m). **(3)** Orgán a osoba uvedená v § 3 písm. e) určí bezpečnostní role přiměřeně podle odstavce 2. **(4)** Manažer kybernetické bezpečnosti je osoba, odpovědná za systém řízení bezpečnosti informací, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s řízením bezpečnosti informací po dobu nejméně tří let. **(5)** Architekt kybernetické bezpečnosti je osoba zajišťující návrh a implementaci bezpečnostních opatření, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s navrhováním bezpečnostní architektury po dobu nejméně tří let. **(6)** Auditor kybernetické bezpečnosti je osoba provádějící audit kybernetické bezpečnosti, která je pro tuto činnost 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 uvedených v odstavci 2 písm. a), b) nebo d). **(7)** Výbor pro řízení kybernetické bezpečnosti je 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. **(8)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona zajistí odborné školení osob, které zastávají bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí podle § 9 odst. 1 písm. b).	**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

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
	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

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
	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.
§ 7 **Stanovení bezpečnostních požadavků pro dodavatele** **(1)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona zavede pravidla pro dodavatele, která zohledňují potřeby řízení bezpečnosti informací, a zohlední je u dodavatelů nebo jiných osob, které se podílejí na rozvoji, provozu nebo zajištění	**§ 8** **Řízení dodavatelů** **(1)** Povinná osoba **a)** stanoví pravidla pro dodavatele, která zohledňují požadavky systému řízení

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému. Rozsah zapojení dodavatelů na rozvoji, provozu nebo zajištění bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému prokazatelně dokumentuje orgán a osoba uvedená v § 3 písm. c) až e) zákona smlouvou, jejíž součástí je ustanovení o bezpečnosti informací. **(2)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona u dodavatelů uvedených v odstavci 1 dále **a)** před uzavřením smlouvy provádí hodnocení rizik podle přílohy č. 2 k této vyhlášce, která jsou spojena s podstatnými dodávkami, **b)** 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, a **c)** 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.	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,

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
	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)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona v rámci řízení bezpečnosti lidských zdrojů **a)** stanoví plán rozvoje bezpečnostního povědomí, který obsahuje formu, obsah a rozsah potřebných školení a určí osoby provádějící realizaci jednotlivých činností, které jsou v plánu uvedeny, **b)** v souladu s plánem rozvoje bezpečnostního povědomí zajistí poučení uživatelů, administrátorů a osob zastávajících bezpečnostní role o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení, **c)** zajistí kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a **d)** zajistí vrácení svěřených aktiv a odebrání přístupových oprávnění při ukončení smluvního vztahu s uživateli, administrátory nebo osobami zastávajícími bezpečnostní role. **(2)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona vede o školení podle odstavce 1 přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly. **(3)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále **a)** stanoví pravidla pro určení osob, které budou zastávat bezpečnostní role, role administrátorů nebo uživatelů,	**§ 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

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
b) hodnotí účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených s prohlubováním bezpečnostního povědomí, **c)** určí pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a **d)** zajistí změnu přístupových oprávnění při změně postavení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role.	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)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona v rámci řízení provozu a komunikací pomocí technických nástrojů uvedených v § 21 až 23 detekuje kybernetické bezpečnostní události, pravidelně vyhodnocuje získané informace a na zjištěné nedostatky reaguje v souladu s § 13. **(2)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona v rámci řízení provozu a komunikací dále zajišťuje bezpečný provoz informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému. Za tímto účelem stanoví provozní pravidla a postupy. **(3)** Provozní pravidla a postupy orgánu a osoby uvedené v § 3 písm. c) a d) zákona obsahují **a)** práva a povinnosti osob zastávajících bezpečnostní role, administrátorů a	**§ 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,

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
uživatelů, **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 pro ochranu přístupu k záznamům o těchto činnostech, **d)** spojení na kontaktní osoby, které jsou určeny jako podpora při řešení neočekávaných systémových nebo technických potíží, **e)** postupy řízení a schvalování provozních změn a **f)** postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů. **(4)** Řízení provozu orgánu a osoby uvedené v § 3 písm. c) až e) zákona spočívá v provádění pravidelného zálohování a prověřování použitelnosti provedených záloh. **(5)** Řízení provozu orgánu a osoby uvedené v § 3 písm. c) a d) zákona spočívá v **a)** zajištění oddělení vývojového, testovacího a produkčního prostředí, **b)** řešení reaktivních opatření vydaných Úřadem tím, že orgán a osoba uvedená v § 3 písm. c) a d) zákona **1.** posoudí očekávané dopady reaktivního opatření na informační systém kritické informační infrastruktury nebo komunikační systém kritické informační infrastruktury a na zavedená bezpečnostní opatření, vyhodnotí možné negativní účinky a bez zbytečného odkladu je oznámí Úřadu a **2.** stanoví způsob rychlého provedení reaktivního opatření, který minimalizuje možné negativní účinky, a určí časový plán jeho provedení. **(6)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona v rámci řízení komunikací **a)** zajišťuje bezpečnost a integritu komunikačních sítí a bezpečnost komunikačních služeb podle § 17, **b)** určí pravidla a postupy pro ochranu informací, které jsou přenášeny	**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.

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
komunikačními sítěmi, **c)** provádí výměnu a předávání informací na základě pravidel stanovených právními předpisy za současného zajištění bezpečnosti informací a tato pravidla dokumentuje a **d)** s ohledem na klasifikaci aktiv provádí výměnu a předávání informací na základě písemných smluv, jejichž součástí je ustanovení o bezpečnosti informací.	
	§ 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.

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
§ 11 **Řízení přístupu a bezpečné chování uživatelů** **(1)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona na základě provozních a bezpečnostních potřeb řídí přístup k informačnímu systému kritické informační infrastruktury, komunikačnímu systému kritické informační infrastruktury a významnému informačnímu systému a přidělí každému uživateli jednoznačný identifikátor. **(2)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona přijme opatření, která slouží k zajištění ochrany údajů, které jsou používány pro přihlášení uživatelů a administrátorů informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému podle § 18 a 19, a která brání ve zneužití těchto údajů neoprávněnou osobou. **(3)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále v rámci řízení přístupu **a)** přidělí přistupujícím aplikacím samostatný identifikátor, **b)** omezí přidělování administrátorských oprávnění, **c)** přiděluje a odebírá přístupová oprávnění v souladu s politikou řízení přístupu, **d)** provádí pravidelné přezkoumání nastavení přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách nebo rolích, **e)** využívá nástroj pro ověřování identity uživatelů podle § 18 a nástroj pro řízení přístupových oprávnění podle § 19 a **f)** zavede bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení, případně i bezpečnostní opatření spojená s využitím technických zařízení, kterými orgán a osoba uvedená v § 3 písm. c) a d) zákona nedisponuje.	§ 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

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
	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.
§ 12 **Akvizice, vývoj a údržba** **(1)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona stanoví 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 zahrne je do projektu akvizice, vývoje a údržby systému. **(2)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále **a)** identifikuje, hodnotí a řídí 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 § 4 odst. 1 písm. a)použijí obdobně, **b)** zajistí bezpečnost vývojového prostředí a zajistí ochranu používaných testovacích dat a **c)** provádí bezpečnostní testování změn informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury před jejich zavedením do provozu.	**§ 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.

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
§ 13 **Zvládání kybernetických bezpečnostních událostí a incidentů** Orgán a osoba uvedená v § 3 písm. c) až e) zákona při zvládání kybernetických událostí a incidentů **a)** přijme 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 vede záznamy, **b)** připraví prostředí pro vyhodnocení oznámených kybernetických bezpečnostních událostí a kybernetických bezpečnostních událostí detekovaných technickými nástroji podle § 21 až 23, provádí jejich vyhodnocení a identifikuje kybernetické bezpečnostní incidenty, **c)** provádí klasifikaci kybernetických bezpečnostních incidentů, přijímá opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu, provádí hlášení kybernetického bezpečnostního incidentu podle § 32 a zajistí sběr věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu, **d)** prošetří a určí příčiny kybernetického bezpečnostního incidentu, vyhodnotí účinnost řešení kybernetického bezpečnostního incidentu a na základě vyhodnocení stanoví nutná bezpečnostní opatření k zamezení opakování řešeného kybernetického bezpečnostního incidentu a **e)** dokumentuje zvládání kybernetických bezpečnostních incidentů.	§ 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

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
	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.
§ 14 **Řízení kontinuity činností** **(1)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona v rámci řízení kontinuity činností stanoví **a)** práva a povinnosti garantů aktiv, administrátorů a osob zastávajících bezpečnostní role, **b)** cíle řízení kontinuity činností formou určení **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, **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, a **3.** dobu obnovení dat jako termínu, ke kterému budou obnovena data po kybernetickém bezpečnostním incidentu, a **c)** strategii řízení kontinuity činností, která obsahuje naplnění cílů podle písmene b). **(2)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále	**§ 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

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
a) vyhodnotí a dokumentuje možné dopady kybernetických bezpečnostních incidentů a posoudí možná rizika související s ohrožením kontinuity činností, **b)** stanoví, aktualizuje a pravidelně testuje plány kontinuity činností informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury, **c)** realizuje opatření pro zvýšení odolnosti informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury vůči kybernetickému bezpečnostnímu incidentu a využívá nástroj pro zajišťování úrovně dostupnosti podle § 26 a **d)** stanoví a aktualizuje postupy pro provedení opatření vydaných Úřadem podle § 13 a 14 zákona, ve kterých zohlední **1.** výsledky hodnocení rizik provedení opatření, **2.** stav dotčených bezpečnostních opatření a **3.** vyhodnocení případných negativních dopadů na provoz a bezpečnost informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury.	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.
§ 15 **Kontrola a audit kritické informační infrastruktury a významných informačních systémů** **(1)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona v rámci kontroly a auditu kritické informační infrastruktury a významných informačních systémů (dále jen „audit kybernetické bezpečnosti“) **a)** posuzuje soulad bezpečnostních opatření s právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k informačnímu systému kritické informační infrastruktury, komunikačnímu systému kritické informační infrastruktury a významnému informačnímu systému a určí opatření pro jeho prosazování a **b)** provádí a dokumentuje pravidelné kontroly dodržování bezpečnostní politiky a	**§ 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,

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
výsledky těchto kontrol zohlední v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik. **(2)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona zajišťuje provedení auditu kybernetické bezpečnosti osobou s odbornou kvalifikací podle § 6 odst. 6, která hodnotí správnost a účinnost zavedených bezpečnostních opatření. **(3)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále pro informační systém kritické informační infrastruktury a komunikační systém kritické informační infrastruktury provádí kontrolu zranitelnosti technických prostředků pomocí automatizovaných nástrojů a jejich odborné vyhodnocení a reaguje na zjištěné zranitelnosti.	**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** **§ 16** **Fyzická bezpečnost** **(1)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona v rámci fyzické bezpečnosti **a)** přijme 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, **b)** přijme 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, a	**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,

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
c) předchází poškození, krádeži nebo zneužití aktiv nebo přerušení poskytování služeb informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému. **(2)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále uplatňuje prostředky fyzické bezpečnosti **a)** pro zajištění ochrany na úrovni objektů a **b)** 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)** 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.	**2.** k zamezení poškození a neoprávněným zásahům a **3.** pro zajištění ochrany na úrovni objektů a v rámci objektů.
§ 17 **Nástroj pro ochranu integrity komunikačních sítí** **(1)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona 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, zavede **a)** řízení bezpečného přístupu mezi vnější a vnitřní sítí, **b)** segmentaci zejména použitím demilitarizovaných zón jako speciálního typu sítě	**§ 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

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
používaného ke zvýšení bezpečnosti aplikací dostupných z vnější sítě a k zamezení přímé komunikace vnitřní sítě s vnější sítí, **c)** kryptografické prostředky (§ 25) pro vzdálený přístup, vzdálenou správu nebo pro přístup pomocí bezdrátových technologií a **d)** opatření pro odstranění nebo blokování přenášených dat, které neodpovídají požadavkům na ochranu integrity komunikační sítě. **(2)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále využívá nástroje pro ochranu integrity vnitřní komunikační sítě, které zajistí její segmentaci.	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.
§ 18 **Nástroj pro ověřování identity uživatelů** **(1)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona používá nástroje pro ověření identity uživatelů a administrátorů informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému. **(2)** 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)** Nástroj pro ověřování identity uživatelů, který používá autentizaci pouze heslem, zajišťuje **a)** minimální délku hesla osm znaků, **b)** minimální složitost hesla tak, že heslo bude obsahovat alespoň 3 z následujících čtyř požadavků **1.** nejméně jedno velké písmeno, **2.** nejméně jedno malé písmeno, **3.** nejméně jednu číslici, nebo **4.** nejméně jeden speciální znak odlišný od požadavků uvedených v bodech 1 až	**§ 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.

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
3, **c)** maximální dobu pro povinnou výměnu hesla nepřesahující sto dnů; tento požadavek není vyžadován pro samostatné identifikátory aplikací. **(4)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále **a)** používá nástroj pro ověření identity, který **1.** zamezí opětovnému používání dříve používaných hesel a neumožní více změn hesla jednoho uživatele během stanoveného období, které musí být nejméně 24 hodin, a **2.** provádí opětovné ověření identity po určené době nečinnosti a **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). **(5)** Nástroj pro ověřování identity uživatelů může být zajištěn i jinými způsoby, než jaké jsou stanoveny v odstavcích 3 až 5, pokud orgán a osoba uvedená v § 3 písm. c) až e) zákona zabezpečí, že používá opatření zajišťující stejnou nebo vyšší úroveň odolnosti hesla.	**(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

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
	bezpečnostního povědomí podle § 9.
§ 19 **Nástroj pro řízení přístupových oprávnění** **(1)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona používá nástroj pro řízení přístupových oprávnění, kterým zajistí řízení oprávnění **a)** pro přístup k jednotlivým aplikacím a datům a **b)** pro čtení dat, pro zápis dat a pro změnu oprávnění. **(2)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále používá nástroj pro řízení přístupových oprávnění, který zaznamenává použití přístupových oprávnění v souladu s bezpečnostními potřebami a výsledky hodnocení rizik	**§ 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.
§ 20 **Nástroj pro ochranu před škodlivým kódem** Orgán a osoba uvedená v § 3 písm. c) až e) zákona pro řízení rizik spojených s působením škodlivého kódu používá 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 **a)** komunikace mezi vnitřní sítí a vnější sítí, **b)** serverů a sdílených datových úložišť a **c)** pracovních stanic, přičemž provádí pravidelnou a účinnou aktualizaci nástroje pro ochranu před škodlivým kódem, jeho definic a signatur.	**§ 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

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
	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.
§ 21 **Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů** **(1)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona používá nástroj pro zaznamenávání činností informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému, který zajistí **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 a **b)** ochranu získaných informací před neoprávněným čtením nebo změnou. **(2)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona dále pomocí nástroje pro zaznamenávání činnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému zaznamenává **a)** přihlášení a odhlášení uživatelů a administrátorů, **b)** činnosti provedené administrátory, **c)** činnosti vedoucí ke změně přístupových oprávnění, **d)** neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů, **e)** zahájení a ukončení činností technických aktiv informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému,	§ 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,

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
f) automatická varovná nebo chybová hlášení technických aktiv, **g)** přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností a **h)** použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení. **(3)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona záznamy činností zaznamenané podle odstavce 2 uchovává nejméně po dobu 3 měsíců. **(4)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona zajišťuje nejméně jednou za 24 hodin synchronizaci jednotného systémového času technických aktiv patřících do informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.	**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.
§ 22 **Nástroj pro detekci kybernetických bezpečnostních událostí** **(1)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona používá nástroj pro detekci kybernetických bezpečnostních událostí, který vychází ze stanovených bezpečnostních potřeb a výsledků hodnocení rizik a který zajistí ověření, kontrolu a případně zablokování komunikace mezi vnitřní komunikační sítí a vnější sítí. **(2)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále používá nástroj pro detekci kybernetických bezpečnostních událostí, které zajistí ověření, kontrolu a případně zablokování komunikace	**§ 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

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
a) v rámci vnitřní komunikační sítě a **b)** serverů patřících do informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury.	**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.
§ 23 **Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí** **(1)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona používá nástroj pro sběr a průběžné vyhodnocení kybernetických bezpečnostních událostí, který v souladu s bezpečnostními potřebami a výsledky hodnocení rizik zajistí **a)** integrovaný sběr a vyhodnocení kybernetických bezpečnostních událostí z informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury, **b)** poskytování informací pro určené bezpečnostní role o detekovaných kybernetických bezpečnostních událostech v informačním systému kritické informační infrastruktury nebo komunikačním systému kritické informační infrastruktury a **c)** nepřetržité vyhodnocování kybernetických bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů, včetně včasného varování určených bezpečnostních rolí. **(2)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále zajistí	**§ 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

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
a) pravidelnou aktualizaci nastavení pravidel pro vyhodnocování kybernetických bezpečnostních událostí a včasné varování, aby byly omezovány případy nesprávného vyhodnocení událostí nebo případy falešných varování, a **b)** 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.	**f)** využívání informací získaných nástrojem pro sběr a vyhodnocení kybernetických bezpečnostních událostí pro optimální nastavení bezpečnostních opatření informačního a komunikačního systému.
§ 24 **Aplikační bezpečnost** **(1)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona provádí bezpečnostní testy zranitelnosti aplikací, které jsou přístupné z vnější sítě, a to před jejich uvedením do provozu a po každé zásadní změně bezpečnostních mechanismů. **(2)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále v rámci aplikační bezpečnosti zajistí trvalou ochranu **a)** aplikací a informací dostupných z vnější sítě před neoprávněnou činností, popřením provedených činností, kompromitací nebo neautorizovanou změnou a **b)** transakcí před jejich nedokončením, nesprávným směrováním, neautorizovanou změnou předávaného datového obsahu, kompromitací, neautorizovaným duplikováním nebo opakováním.	**§ 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.
§ 25 **Kryptografické prostředky** **(1)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona **a)** pro používání kryptografické ochrany stanoví **1.** úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu a **2.** pravidla kryptografické ochrany informací při přenosu po komunikačních sítích nebo při uložení na mobilní zařízení nebo vyměnitelné technické nosiče dat a **b)** v souladu s bezpečnostními potřebami a výsledky hodnocení rizik používá	**§ 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,

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
kryptografické prostředky, které zajistí ochranu důvěrnosti a integrity předávaných nebo ukládaných dat a průkaznou identifikaci osoby za provedené činnosti. **(2)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále **a)** stanoví pro používání kryptografických prostředků systém správy klíčů, který zajistí generování, distribuci, ukládání, archivaci, změny, ničení, kontrolu a audit klíčů, a **b)** používá 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.	**c)** prosazuje bezpečné nakládání s kryptografickými prostředky a **d)** zohledňuje doporučení v oblasti kryptografických prostředků vydaná Úřadem, zveřejněná na jeho internetových stránkách.
§ 26 **Nástroj pro zajišťování úrovně dostupnosti** **(1)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona v souladu s bezpečnostními potřebami a výsledky hodnocení rizik používá nástroj pro zajišťování úrovně dostupnosti informací. **(2)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona používá nástroj pro zajišťování úrovně dostupnosti informací, který zajistí **a)** dostupnost informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury pro splnění cílů řízení kontinuity činností, **b)** odolnost informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury vůči kybernetickým bezpečnostním incidentům, které by mohly snížit dostupnost, a **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.	**§ 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.

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
§ 27 **Bezpečnost průmyslových a řídicích systémů** Orgán a osoba uvedená v § 3 písm. c) a d) zákona pro bezpečnost průmyslových a řídicích systémů, které jsou informačním systémem kritické informační infrastruktury nebo komunikačním systémem kritické informační infrastruktury anebo jsou jejich součástí, používá nástroje, které zajistí **a)** omezení fyzického přístupu k síti a zařízením průmyslových a řídicích systémů, **b)** omezení propojení a vzdáleného přístupu k síti průmyslových a řídicích systémů, **c)** ochranu jednotlivých technických aktiv průmyslových a řídicích systémů před využitím známých zranitelností a **d)** obnovení chodu průmyslových a řídicích systémů po kybernetickém bezpečnostním incidentu.	§ 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.

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
§ 5 **Bezpečnostní politika** **(1)** Orgán a osoba uvedená v § 3 písm. c) a d) zákona stanoví bezpečnostní politiku v oblastech **a)** systém řízení bezpečnosti informací, **b)** organizační bezpečnost, **c)** řízení vztahů s dodavateli, **d)** klasifikace aktiv, **e)** bezpečnost lidských zdrojů, **f)** řízení provozu a komunikací, **g)** řízení přístupu, **h)** bezpečné chování uživatelů, **i)** zálohování a obnova, **j)** bezpečné předávání a výměna informací, **k)** řízení technických zranitelností, **l)** bezpečné používání mobilních zařízení, **m)** poskytování a nabývání licencí programového vybavení a informací, **n)** dlouhodobé ukládání a archivace informací, **o)** ochrana osobních údajů, **p)** fyzická bezpečnost, **q)** bezpečnost komunikační sítě, **r)** ochrana před škodlivým kódem, **s)** nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí, **t)** využití a údržba nástroje pro sběr a vyhodnocení kybernetických	**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.

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
bezpečnostních událostí a **u)** používání kryptografické ochrany. **(2)** Orgán a osoba uvedená v § 3 písm. e) zákona stanoví bezpečnostní politiku v oblastech **a)** systém řízení bezpečnosti informací, **b)** organizační bezpečnost, **c)** řízení dodavatelů, **d)** klasifikace aktiv, **e)** bezpečnost lidských zdrojů, **f)** řízení provozu a komunikací, **g)** řízení přístupu, **h)** bezpečné chování uživatelů, **i)** zálohování a obnova, **j)** poskytování a nabývání licencí programového vybavení a informací, **k)** ochrana osobních údajů, **l)** používání kryptografické ochrany, **m)** ochrana před škodlivým kódem a **n)** nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí. **(3)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona pravidelně hodnotí účinnost bezpečnostní politiky a aktualizuje ji. **HLAVA III** **BEZPEČNOSTNÍ DOKUMENTACE** **§ 28** **Bezpečnostní dokumentace**	

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
(1) Orgán a osoba uvedená v § 3 písm. c) a d) zákona vede a aktualizuje bezpečnostní dokumentaci, která obsahuje **a)** bezpečnostní politiku podle § 5 odst. 1, **b)** zprávy z auditu kybernetické bezpečnosti podle § 3 odst. 1 písm. f), **c)** zprávy z přezkoumání systému řízení bezpečnosti informací podle § 3 odst. 1 písm. g), **d)** metodiku pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik, **e)** zprávu o hodnocení aktiv a rizik, **f)** prohlášení o aplikovatelnosti, **g)** plán zvládání rizik, **h)** plán rozvoje bezpečnostního povědomí podle § 9 odst. 1 písm. a), **i)** zvládání kybernetických bezpečnostních incidentů podle § 13 písm. e), **j)** strategii řízení kontinuity činností podle § 14 odst. 1 písm. c) a **k)** přehled právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků podle § 15 odst. 1 písm. a). **(2)** Orgán a osoba uvedená v § 3 písm. e) zákona vede a aktualizuje bezpečnostní dokumentaci, která obsahuje **a)** bezpečnostní politiku podle § 5 odst. 2, **b)** metodiku pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik podle § 4 odst. 2 písm. a), **c)** zprávu o hodnocení aktiv a rizik podle § 4 odst. 2 písm. b) a c), **d)** prohlášení o aplikovatelnosti podle § 4 odst. 2 písm. d), **e)** plán zvládání rizik podle § 4 odst. 2 písm. e), **f)** plán rozvoje bezpečnostního povědomí podle § 9 odst. 1 písm. a), **g)** zvládání kybernetických bezpečnostních incidentů podle § 13 písm. e), **h)** strategii řízení kontinuity činností podle § 14 odst. 1 písm. c) a	

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
i) přehled právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků podle § 15 odst. 1 písm. a). **(3)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona vede bezpečnostní dokumentaci tak, aby záznamy o provedených činnostech byly úplné, čitelné, snadno identifikovatelné a aby se daly snadno vyhledat. Opatření potřebná k identifikaci, uložení, ochraně, vyhledání, době platnosti a uspořádání záznamů o provedených činnostech dokumentuje. **(4)** Doporučená struktura bezpečnostní dokumentace je stanovena v příloze č. 4 k této vyhlášce.	
§ 29 **Prokázání certifikace** Orgán a osoba uvedená v § 3 písm. c) až e) zákona, jejíž informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém je zcela zahrnut do rozsahu systému řízení bezpečnosti informací, který byl certifikován podle příslušné technické normy[1]) akreditovaným certifikačním orgánem, a která vede dokumenty obsahující **a)** popis rozsahu systému řízení bezpečnosti informací, **b)** prohlášení politiky a cílů systému řízení bezpečnosti informací, **c)** popis použité metody hodnocení rizik a zprávu o hodnocení rizik, **d)** prohlášení o aplikovatelnosti, **e)** certifikát systému řízení bezpečnosti informací splňující požadavky příslušné technické normy zabývající se bezpečností informací[1]), **f)** záznam o přezkoumání systému řízení bezpečnosti informací včetně souvisejících vstupů a výstupů přezkoumání a **g)** zprávu z auditů provedených certifikačním orgánem včetně příslušných záznamů o nápravě zjištěných neshod s příslušnou normou, splňuje požadavky na zavedení bezpečnostních opatření podle zákona a této	

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
vyhlášky.	
ČÁST TŘETÍ **KYBERNETICKÝ BEZPEČNOSTNÍ INCIDENT** **§ 30** **Typy kybernetických bezpečnostních incidentů** **(1)** Podle příčiny jsou kybernetické bezpečnostní incidenty rozděleny do následujících typů **a)** kybernetický bezpečnostní incident způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do systému nebo k omezení dostupnosti služeb, **b)** kybernetický bezpečnostní incident způsobený škodlivým kódem, **c)** kybernetický bezpečnostní incident způsobený překonáním technických opatření, **d)** kybernetický bezpečnostní incident způsobený porušením organizačních opatření, **e)** kybernetický bezpečnostní incident spojený s projevem trvale působících hrozeb a **f)** ostatní kybernetické bezpečnostní incidenty způsobené kybernetickým útokem. **(2)** Podle dopadu jsou kybernetické bezpečnostní incidenty rozděleny do následujících typů **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).	**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

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
	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.
§ 31 **Kategorie kybernetických bezpečnostních incidentů** **(1)** Pro potřeby zvládání kybernetických bezpečnostních incidentů se podle následků a negativních projevů kybernetické bezpečnostní incidenty dělí do následujících kategorií **a)** Kategorie III - velmi závažný 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 - závažný kybernetický bezpečnostní incident, při kterém je	

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření kybernetického incidentu včetně minimalizace vzniklých škod. **c)** Kategorie I - méně závažný 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. **(2)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona při kategorizaci jednotlivých kybernetických bezpečnostních incidentů podle odstavce 1 zohlední **a)** důležitost dotčených aktiv informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému, **b)** dopady na poskytované služby informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury, nebo významného informačního systému, **c)** dopady na služby poskytované jinými informačními systémy kritické informační infrastruktury, komunikačními systémy kritické informační infrastruktury, nebo významnými informačními systémy a **d)** předpokládané škody a další dopady.	
§ 32 **Forma a náležitosti hlášení kybernetických bezpečnostních incidentů** **(1)** Orgán a osoba uvedená v § 3 písm. c) až e) zákona hlásí kybernetický bezpečnostní incident **a)** v elektronické podobě prostřednictvím **1.** elektronického formuláře zveřejněného na internetových stránkách Úřadu, **2.** emailu na adresu elektronické pošty Úřadu určené pro příjem hlášení kybernetických bezpečnostních incidentů, zveřejněné na internetových stránkách	**§ 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,

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
Úřadu, **3.** datové zprávy do datové schránky Úřadu, nebo **4.** prostřednictvím určeného datového rozhraní, jehož popis je zveřejněn na internetových stránkách Úřadu, anebo **b)** v listinné podobě na adresu Národního centra kybernetické bezpečnosti, zveřejněné na internetových stránkách Úřadu. **(2)** Hlášení v listinné podobě se zasílá pouze v případech, kdy nelze využít žádný ze způsobů uvedených v odstavci 1 písm. a). **(3)** Náležitosti hlášení kybernetického bezpečnostního incidentu jsou uvedeny v příloze č. 5 k této vyhlášce.	**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** Orgán a osoba uvedená v § 3 písm. c) až e) zákona oznámí provedení reaktivního opatření a jeho výsledek na formuláři, jehož vzor je uveden v příloze č. 6 k této vyhlášce.	**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

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
	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** Orgán a osoba uvedená v § 3 zákona oznamuje kontaktní údaje na formuláři, jehož vzor je uveden v příloze č. 7 k této vyhlášce. Orgán a osoba uvedená v § 3 písm. c) až e) zákona oznamuje kontaktní údaje formou uvedenou v § 32 odst. 1 písm. a).	**§ 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

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
	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

Vyhláška č. 316/2014 Sb.	Vyhláška č. 82/2018 Sb.
	kybernetické bezpečnosti).
ČÁST PÁTÁ **ÚČINNOST** **§ 35** Tato vyhláška nabývá účinnosti dnem 1. ledna 2015.	**§ 37** **Účinnost** Tato vyhláška nabývá účinnosti dnem vyhlášení.
Ředitel: Ing. Navrátil v. r.	Ředitel: Ing. Navrátil v. r.