Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Manažerské shrnutí

Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností navazuje na ustanovení v novém Zákoně o kybernetické bezpečnosti, které říká, že prováděcí právní předpis stanoví bezpečnostní opatření pro poskytovatele regulované služby odpovídající jeho režimu. Každý poskytovatel regulované služby má stanoven jen jeden režim pro všechny své služby a proto tuto vyhlášku použijí jen ti poskytovatelé regulované služby, jejichž výsledný režim je vyšší.

Obsah této vyhlášky vychází ze současné vyhlášky o kybernetické bezpečnosti, dochází jen k dílčím úpravám a reflexi zkušeností.

V Části Třetí navazuje na ustanovení v novém Zákoně o kybernetické bezpečnosti o lokalizaci dat v případě poskytovatele regulované služby v režimu vyšších povinností.

Tento dokument slouží jako rozpracované teze budoucí vyhlášky a je proto podkladem k další diskuzi. Může se měnit a to v závislosti jak na obsahu připomínek odborné veřejnosti, tak na obsahu připomínek v průběhu legislativního procesu.

Návrh

VYHLÁŠKA

ze dne dd.mm.rrrr,

o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností

Národní úřad pro kybernetickou a informační bezpečnost stanoví podle § X zákona č. X, o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti):

ČÁST PRVNÍ
ÚVODNÍ USTANOVENÍ

§ 1
Předmět právní úpravy

Tato vyhláška zapracovává příslušný předpis Evropské unie[1] a pro poskytovatele regulované služby v režimu vyšších povinností (dále jen „povinná osoba“) upravuje

[1] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2).

a) obsah a rozsah bezpečnostních opatření a

b) informace a data, na která se vztahuje povinnost povinné osoby zajistit jejich zpracování na vymezeném území a tato vymezená území.

§ 2
Vymezení pojmů

Pro účely této vyhlášky se rozumí

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

b) akceptovatelným rizikem riziko, které je přijatelné pro povinnou osobu,

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

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

e) privilegovaným uživatelem uživatel či osoba, jehož činnost na technickém aktivu může mít významný dopad na bezpečnost regulované služby,

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

g) řízením rizik systematický proces zahrnující hodnocení rizik, zavádění bezpečnostních opatření ke zvládání rizik a komunikaci rizik,

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

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

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

k) významnou změnou změna, která má nebo může mít vliv na kybernetickou bezpečnost a je určena na základě stanovených pravidel, postupů a kritérií.

ČÁST DRUHÁ
BEZPEČNOSTNÍ OPATŘENÍ

§ 3

Povinná osoba zavede a provádí bezpečnostní opatření podle tohoto právního předpisu v rozsahu řízení kybernetické bezpečnosti stanoveného podle § X zákona (dále jen „stanovený rozsah“).

HLAVA I
ORGANIZAČNÍ OPATŘENÍ

§ 4
Systém řízení bezpečnosti informací

1) Povinná osoba v rámci systému řízení bezpečnosti informací
   a) stanoví cíle systému řízení bezpečnosti informací směřující k zajištění bezpečnosti regulované služby,
   b) na základě cílů systému řízení bezpečnosti informací, bezpečnostních potřeb a hodnocení rizik zavede přiměřená bezpečnostní opatření směřující k zajištění bezpečnosti regulované služby,
   c) řídí rizika podle § 9,
   d) vytvoří a schválí bezpečnostní politiku ve vztahu k řízení kybernetické bezpečnosti, která obsahuje hlavní zásady, cíle systému řízení bezpečnosti informací, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací, a na základě bezpečnostních potřeb a výsledků hodnocení rizik stanoví bezpečnostní politiku a bezpečnostní dokumentaci v dalších oblastech podle § 7,
   e) zajistí provedení auditu kybernetické bezpečnosti podle § 17,
   f) zajistí vyhodnocení účinnosti systému řízení bezpečnosti informací alespoň jednou ročně, které obsahuje
      1. vyhodnocení cílů systému řízení bezpečnosti informací směřujících k zajištění bezpečnosti regulované služby,
      2. posouzení naplňování plánu zvládání rizik zpracovaného podle § 9 písm. g),
      3. hodnocení stavu systému řízení bezpečnosti informací včetně revize hodnocení rizik,
      4. posouzení výsledků provedených auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti,
      5. výsledky předchozích hodnocení účinnosti systému řízení bezpečnosti informací provedených podle tohoto písmena,
      6. posouzení dopadů kybernetických bezpečnostních incidentů na poskytované služby podle § 16 a na oblast kybernetické bezpečnosti a
      7. posouzení změn, které mohou mít negativní dopad na systém řízení bezpečnosti informací podle § 12,
   g) na základě vyhodnocení účinnosti systému řízení bezpečnosti informací podle písmena f) zpracuje zprávu o přezkoumání systému řízení bezpečnosti informací,
   h) průběžně identifikuje a následně podle § 12 řídí významné změny,
   i) aktualizuje systém řízení bezpečnosti informací a příslušnou dokumentaci na základě
      1. zjištění auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti,
      2. výsledků vyhodnocení účinnosti systému řízení bezpečnosti informací,

3. dopadů kybernetických bezpečnostních incidentů na poskytované služby a
4. v souvislosti s prováděnými významnými změnami,

j) řídí provoz a zdroje systému řízení bezpečnosti informací a zaznamenává činnosti spojené se systémem řízení bezpečnosti informací a řízením rizik a
k) stanoví proces řízení výjimek z pravidel stanovených podle písm. e).

2) Povinná osoba v případě neplnění povinnosti řízení rizik podle odstavce 1 písm. c)
a) zavede všechna bezpečnostní opatření požadovaná touto vyhláškou,
b) zpracuje o bezpečnostních opatřeních podle písm. a),
1. prohlášení o aplikovatelnosti podle § 9 odst. 1 písm. f) a
2. plán zvládání rizik přiměřeně podle § 9 odst. 1 písm. g),
c) zohlední v plánu zvládání rizik
1. významné změny,
2. změny stanoveného rozsahu podle § X zákona,
3. protiopatření podle § X zákona,
4. kybernetické bezpečnostní incidenty, včetně dříve řešených,
5. výsledky auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti a
6. výsledky penetračního testování a skenování zranitelností,
d) v souladu s plánem zvládání rizik zavádí bezpečnostní opatření.

§ 5
Povinnosti vrcholového vedení

1) Vrcholové vedení s ohledem na systém řízení bezpečnosti informací
a) se prokazatelně účastní školení podle § 11 odst. 3 písm. a),
b) zajistí stanovení bezpečnostní politiky a cílů systému řízení bezpečnosti informací podle § 4, slučitelných se strategickým směřováním povinné osoby,
c) zajistí integraci systému řízení bezpečnosti informací do procesů povinné osoby,
d) zajistí dostupnost zdrojů potřebných pro systém řízení bezpečnosti informací,
e) informuje zaměstnance o významu systému řízení bezpečnosti informací a významu dosažení shody s jeho požadavky se všemi dotčenými stranami,
f) zajistí podporu k dosažení cílů systému řízení bezpečnosti informací,
g) vede zaměstnance k rozvíjení efektivity systému řízení bezpečnosti informací a podporuje je při tomto rozvíjení,
h) se podílí na vypracování analýzy dopadů podle § 16,
i) prosazuje neustálé zlepšování systému řízení bezpečnosti informací,
j) podporuje osoby zastávající bezpečnostní role při prosazování kybernetické bezpečnosti v oblastech jejich odpovědnosti,
k) zajistí stanovení pravidel pro určení administrátorů a osob, které budou zastávat bezpečnostní role,
l) zajistí, aby byla zachována mlčenlivost administrátorů a osob zastávajících bezpečnostní role,

m) pro osoby zastávající bezpečnostní role zajistí příslušné pravomoci a zdroje včetně rozpočtových prostředků k naplňování jejich rolí a plnění souvisejících úkolů a
n) zajistí testování plánů kontinuity činností, plánů obnovy a procesů spojených se zvládáním kybernetických bezpečnostních incidentů.

2) Vrcholové vedení se prokazatelně seznamuje se
   a) zprávou o přezkoumání systému řízení bezpečnosti informací,
   b) zprávou o hodnocení rizik,
   c) výsledky analýzy dopadů v souladu s § 16 a
   d) výsledky auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti.
3) Vrcholové vedení v rámci systému řízení bezpečnosti informací určí složení výboru pro řízení kybernetické bezpečnosti, bezpečnostní role, jejich práva a povinnosti související se systémem řízení bezpečnosti informací.
4) Jednání výboru pro řízení kybernetické bezpečnosti probíhají v pravidelném intervalu a o jejich průběhu je veden dokumentovaný záznam.
5) 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.
6) Vrcholové vedení určí osobu, která bude zastávat bezpečnostní roli
   a) manažera kybernetické bezpečnosti,
   b) architekta kybernetické bezpečnosti,
   c) garanta aktiva a
   d) auditora kybernetické bezpečnosti.
7) Vrcholové vedení zajistí zastupitelnost bezpečnostních rolí uvedených v odstavci 6 písm. a) a b).

§ 6
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,

c) nesmí být pověřen výkonem rolí odpovědných za provoz regulované služby.

2) Architekt kybernetické bezpečnosti je bezpečnostní role odpovědná za zajištění návrhu implementace bezpečnostních opatření tak, aby byla zajištěna bezpečná architektura regulované služby, 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
Řízení bezpečnostní politiky a bezpečnostní dokumentace

1) Povinná osoba v rámci řízení bezpečnostní politiky a bezpečnostní dokumentace
   a) stanoví bezpečnostní politiku a vede bezpečnostní dokumentaci zahrnující oblasti uvedené v příloze č. 5 k této vyhlášce a
   b) v provozní dokumentaci stanoví pravidla a postupy, které zohledňují relevantní oblasti z bezpečnostní politiky a bezpečnostní dokumentace.
2) Povinná osoba dodržuje pravidla a postupy stanovené podle odstavce 1.
3) Povinná osoba pravidelně přezkoumává bezpečnostní politiku a bezpečnostní dokumentaci, zajistí jejich aktuálnost a zohlednění jejich relevantních oblastí v provozní dokumentaci.
4) Povinná osoba určí osobu odpovědnou za pravidelný přezkum a aktualizaci bezpečnostní politiky, bezpečnostní dokumentace a zohlednění jejich relevantních oblastí v provozní dokumentaci podle odstavce 3.
5) Bezpečnostní politika a bezpečnostní dokumentace musí být řízeny tak, aby byly
   a) dostupné v elektronické nebo listinné podobě,
   b) komunikovány v rámci povinné osoby,
   c) přiměřeně dostupné dotčeným stranám,
   d) chráněny z pohledu důvěrnosti, integrity a dostupnosti a

e) vedeny tak, aby informace v nich obsažené byly úplné, čitelné, správné, snadno identifikovatelné a vyhledatelné.

§ 8
Řízení aktiv

Povinná osoba v souladu s provedenou identifikací a evidencí aktiv

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

b) určí a eviduje garanty aktiv,

c) hodnotí primární aktiva z hlediska důvěrnosti, integrity a dostupnosti a zařadí je do jednotlivých úrovní podle písm. a),

d) v rámci hodnocení primárních aktiv posuzuje alespoň oblasti uvedené v příloze č. 1 k této vyhlášce,

e) identifikuje a eviduje relevantní vazby mezi aktivy,

f) hodnotí podpůrná aktiva a zohledňuje přitom zejména vazby na primární aktiva a

g) pro jednotlivé úrovně aktiv podle písmena a) stanovuje a zavádí pravidla ochrany nutná pro zabezpečení jejich důvěrnosti, dostupnosti a integrity, které obsahují zejména

   i) přípustné způsoby používání aktiv,

   ii) pravidla pro manipulaci s aktivy,

   iii) pravidla pro klasifikaci informací,

   iv) pravidla pro označování aktiv,

   v) pravidla správy výměnných médií,

   vi) pravidla pro bezpečné elektronické sdílení a fyzické přenášení aktiv a

   vii) pravidla pro určení způsobu likvidace informací a dat a jejich kopií a likvidaci technických aktiv, která jsou nosiči informací a dat s ohledem na úroveň aktiv v souladu s přílohou č. 4 k této vyhlášce.

§ 9
Řízení rizik

1) Povinná osoba v rámci řízení rizik v návaznosti na § 8

   a) stanoví metodiku pro identifikaci a hodnocení rizik, včetně stanovení kritérií pro akceptovatelnost rizik,

   b) při identifikaci rizik 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 alespoň jednou ročně a při významných změnách,

d) při hodnocení rizik zohlední relevantní hrozby a zranitelnosti podle písmena b) a posoudí možné dopady na aktiva; tato rizika hodnotí alespoň v rozsahu přílohy č. 2 k této vyhlášce,
e) na základě provedeného hodnocení rizik podle písmena d) zpracuje zprávu o hodnocení rizik,
f) zpracuje na základě bezpečnostních potřeb a výsledků hodnocení rizik prohlášení o aplikovatelnosti, které obsahuje přehled všech bezpečnostních opatření požadovaných touto vyhláškou, která
   1. nebyla aplikována, včetně odůvodnění a přehledu přijatých náhradních bezpečnostních opatření,
   2. byla aplikována, včetně způsobu plnění,
g) na základě provedeného hodnocení rizik podle písmena d) zpracuje plán zvládání rizik, který obsahuje
   1. popis bezpečnostních opatření,
   2. cíle a přínosy bezpečnostních opatření pro zvládání jednotlivých rizik,
   3. určení osoby zajišťující zavedení bezpečnostních opatření pro zvládání rizik,
   4. předpokládané lidské, finanční a technické zdroje pro zavedení bezpečnostních opatření,
   5. požadovaný termín zavedení bezpečnostních opatření,
   6. popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními a
   7. způsob realizace bezpečnostních opatření,
h) při hodnocení rizik a v plánu zvládání rizik zohlední
   1. významné změny,
   2. změny stanoveného rozsahu podle § X zákona,
   3. protiopatření podle § X zákona,
   4. kybernetické bezpečnostní incidenty, včetně dříve řešených,
   5. výsledky auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti,
   6. výsledky penetračního testování a skenování zranitelností a
   7. upozornění na riziko spojené s dodavatelem podle § X zákona.

2) Povinná osoba v souladu s plánem zvládání rizik zavádí bezpečnostní opatření.
3) Řízení rizik může být zajištěno i jinými způsoby, než jak je stanoveno v odstavci 1 písm. d), pokud povinná osoba zajistí stejnou nebo vyšší úroveň procesu řízení rizik.

§ 10
Řízení dodavatelů

1) Povinná osoba
   a) stanoví pravidla pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací,
   b) seznamuje své dodavatele s pravidly podle písmena a) a vyžaduje plnění těchto pravidel,

c) identifikuje a eviduje své významné dodavatele,
d) prokazatelně písemně informuje své významné dodavatele o jejich evidenci podle písmena c).
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. d) jsou
a) identifikace povinné osoby,
b) identifikace regulované služby,
c) identifikace významného dodavatele,
d) vyrozumění o skutečnosti, že dodavatel je pro povinnou osobu významným dodavatelem a
e) obsah pravidel podle odstavce 1 písm. a).

§ 11
Bezpečnost lidských zdrojů

1) Povinná osoba v rámci řízení bezpečnosti lidských zdrojů 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 včetně formy, obsahu a rozsahu poučení a školení podle odstavce 2.
2) Povinná osoba zahrne do plánu rozvoje bezpečnostního povědomí
a) poučení vrcholového vedení o jeho povinnostech, o bezpečnostní politice zejména v oblastech systému řízení bezpečnosti informací a řízení rizik,
b) poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice,
c) potřebná teoretická i praktická školení uživatelů, administrátorů a osob zastávajících bezpečnostní role,
d) pravidla tvorby bezpečných hesel v souladu s § 20,

e) relevantní témata uvedená v příloze č. 8 této vyhlášky.

3) Povinná osoba v rámci řízení bezpečnosti lidských zdrojů
   a) v souladu s plánem rozvoje bezpečnostního povědomí zajistí poučení vrcholového vedení o jeho povinnostech, o bezpečnostní politice zejména v oblasti systému řízení bezpečnosti informací a řízení rizik formou vstupních a pravidelných školení,
   b) 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,
   c) 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,
   d) v souladu s plánem rozvoje bezpečnostního povědomí zajistí pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní,
   e) určí osoby odpovědné za realizaci jednotlivých činností, které jsou v plánu rozvoje bezpečnostního povědomí uvedeny,
   f) hodnotí účinnost plánu rozvoje bezpečnostního povědomí, provedených poučení, školení a dalších činností spojených se zlepšováním bezpečnostního povědomí,
   g) zajistí kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role,
   h) určí pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a
   i) v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role zajistí předání odpovědností.

4) Povinná osoba vede o poučení a školení podle odstavce 3 přehledy, které obsahují předmět poučení a školení včetně seznamu osob, které poučení a školení absolvovaly.

§ 12
Řízení změn

1) Povinná osoba v rámci řízení změn u aktiv
   a) identifikuje změny, které mají nebo mohou mít vliv na kybernetickou bezpečnost,
   b) stanoví pravidla, postupy a kritéria pro určení významných změn a
   c) u změn identifikovaných podle písmene a) určuje významné změny v souladu s písmenem b).
2) Povinná osoba u významných změn
   a) dokumentuje jejich řízení,
   b) provádí hodnocení rizik,

c) přijímá bezpečnostní opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami,
d) aktualizuje bezpečnostní a provozní dokumentaci,
e) zajistí jejich testování před uvedením do provozu a
f) zajistí možnost navrácení do původního stavu.

3) Povinná osoba na základě výsledků hodnocení rizik podle odstavce 2 písm. b) rozhoduje o provedení penetračního testování; pokud rozhodne o provedení penetračního testování, postupuje podle § 25 odst. 6 této vyhlášky.

§ 13
Akvizice, vývoj a údržba

Povinná osoba v souvislosti s plánovanou akvizicí, vývojem a údržbou aktiv

a) řídí rizika podle § 9,
b) řídí významné změny podle § 12,
c) stanoví bezpečnostní požadavky v souladu s touto vyhláškou a vlastními bezpečnostními potřebami,
d) zahrne bezpečnostní požadavky stanovené podle písmene c) do projektu akvizice, vývoje a údržby,
e) dodržuje a vymáhá dodržování požadavků stanovených podle písmene c),
f) zajistí oddělení provozního, zálohovacího, vývojového, testovacího a jiných specifických prostředí, a zajistí ochranu informací a dat se v nich vyskytujících,
g) je-li cílem provedení akvizice nebo vývoje technické aktivum využívající autentizační mechanizmus, zejména za účelem ověření identity uživatelů nebo administrátorů, plní požadavky podle § 20 odst. 3 a
h) je-li cílem provedení akvizice nebo vývoje technické aktivum užívající kryptografické algoritmy, plní požadavky podle § 26 odst. 1 písm. a) a odst. 3 písm. a).

§ 14
Řízení přístupu

1) Povinná osoba na základě bezpečnostních a provozních potřeb řídí přístup k aktivům a přijímá bezpečnostní opatření, která slouží k zajištění ochrany přístupových a autentizačních údajů, které jsou používány pro ověření identity podle § 20 a § 21.
2) Povinná osoba dále v rámci řízení přístupu k aktivům
   a) řídí přístup na základě skupin a rolí,
   b) přidělí každému uživateli a administrátorovi přistupujícímu k aktivům přístupová práva a oprávnění a jedinečný identifikátor,
   c) řídí identifikátory, přístupová práva a oprávnění účtů technických aktiv,
   d) zavádí bezpečnostní opatření pro řízení přístupu technických aktiv k jiným aktivům,

e) zavádí bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení a jiných obdobných technických aktiv, popřípadě i bezpečnostní opatření spojená s využitím technických aktiv, která povinná osoba nemá ve své správě,
f) omezí přidělování administrátorských a privilegovaných oprávnění na úroveň nezbytně nutnou k výkonu náplně práce,
g) omezí a kontroluje používání programových prostředků a vybavení, které mohou být schopné překonat systémové nebo aplikační kontroly,
h) prosazuje, aby byla při používání privátních autentizačních informací a mechanismů dodržována stanovená pravidla a postupy,
i) přiděluje a odebírá přístupová oprávnění v souladu s politikou řízení přístupu,
j) provádí pravidelné přezkoumání veškerých přístupových oprávnění včetně rozdělení do skupin a rolí,
k) zajistí bezodkladné odebrání nebo změnu přístupových oprávnění při změně pozice nebo zařazení na základě skupin a rolí,
l) zajistí bezodkladné odebrání nebo změnu přístupových oprávnění při ukončení nebo změně smluvního vztahu,
m) dokumentuje přidělování a odebírání přístupových oprávnění a
n) využívá nástroj pro správu a ověřování identity podle § 20 a nástroj pro řízení přístupových oprávnění podle § 21.

§ 15
Zvládání kybernetických bezpečnostních událostí a incidentů

1) Povinná osoba v rámci zvládání kybernetických bezpečnostních událostí a incidentů
   a) zavede procesy, pravidla a postupy pro detekci, zaznamenávání a vyhodnocování kybernetických bezpečnostních událostí v souladu s § 22, § 23 a § 24 a zvládání kybernetických bezpečnostních incidentů,
   b) přidělí odpovědnosti pro
      1. detekci, zaznamenávání a vyhodnocování kybernetických bezpečnostních událostí a
      2. koordinaci a zvládání kybernetických bezpečnostních incidentů,
   c) definuje a dodržuje pravidla a postupy pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu,
   d) zajistí detekci kybernetických bezpečnostních událostí podle § 22,
   e) zajistí, že uživatelé, administrátoři, osoby zastávající bezpečnostní role, další zaměstnanci a dodavatelé budou oznamovat neobvyklé chování technických aktiv a podezření na jakékoliv zranitelnosti,
   f) zajistí posuzování kybernetických bezpečnostních událostí, při kterém musí být rozhodnuto, zda mají být klasifikovány jako kybernetické bezpečnostní incidenty,

g) zajistí zvládání kybernetických bezpečnostních incidentů podle stanovených postupů,
h) přijímá bezpečnostní opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu,
i) hlásí kybernetické bezpečnostní incidenty podle § X zákona,
j) vede záznamy o kybernetických bezpečnostních incidentech a o jejich zvládání,
k) prošetří a určí příčiny kybernetického bezpečnostního incidentu a
l) 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 dále při detekci a vyhodnocování kybernetických bezpečnostních událostí používá nástroje podle § 22 a § 24.

§ 16
Řízení kontinuity činností

Povinná osoba v rámci řízení kontinuity činností

a) stanoví metodiku pro provedení analýzy dopadů,
b) pomocí analýzy dopadů vyhodnotí a dokumentuje možné dopady kybernetických bezpečnostních incidentů a zohlední hodnocení rizik podle § 9, v rámci kterého posoudí možná rizika související s ohrožením kontinuity činností,
c) na základě výstupů analýzy dopadů a hodnocení rizik podle písmene b) stanoví cíle řízení kontinuity činností formou určení
    i) minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu regulované služby,
    ii) doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb regulované služby a
    iii) 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) a stanoví práva a povinnosti administrátorů a osob zastávajících bezpečnostní role,
e) vypracuje, aktualizuje a pravidelně testuje plány kontinuity činností a plány obnovy související s poskytováním regulované služby a
f) realizuje bezpečnostní opatření pro zvýšení odolnosti podle § 27.

§ 17
Audit kybernetické bezpečnosti

1) Povinná osoba stanoví plán provádění auditu kybernetické bezpečnosti.
2) Povinná osoba v rámci auditu kybernetické bezpečnosti

a) posuzuje zda byly zavedeny bezpečnostní opatření požadované zákonem o kybernetické bezpečnosti a touto vyhláškou,
b) posuzuje soulad zavedených bezpečnostních opatření s právními předpisy, vnitřními předpisy, jinými předpisy, smluvními závazky a nejlepší praxí vztahujícími se k regulované službě a
c) provádí a dokumentuje audit dodržování pravidel a postupů stanovených v bezpečnostní politice, včetně přezkoumání technické shody a dříve stanovených nápravných opatření podle odstavce 4.

3) Povinná osoba zohlední výsledky auditu kybernetické bezpečnosti podle odstavce 2 v
a) plánu zvládání rizik,
b) prohlášení o aplikovatelnosti a
c) plánu rozvoje bezpečnostního povědomí.
4) Povinná osoba stanoví případná nápravná opatření pro splnění požadavků podle odstavce 2.
5) Audit kybernetické bezpečnosti podle odstavce 2 je prováděn
a) při významných změnách, v rámci jejich rozsahu,
b) v pravidelných intervalech alespoň po 2 letech a
c) v souladu s plánem auditu kybernetické bezpečnosti.
6) Není-li v odůvodněných případech možné provést audit v intervalu podle odstavce 5 písm. b) v celém rozsahu podle odstavce 2, je možné audit kybernetické bezpečnosti provádět průběžně po systematických celcích. V takovém případě je nutno audit v celém rozsahu podle odstavce 2 provést nejpozději do 5 let.
7) Audit kybernetické bezpečnosti musí být prováděn osobou vyhovující podmínkám stanoveným v § 6 odst. 4, která nezávisle hodnotí správnost a účinnost zavedených bezpečnostních opatření.

HLAVA II
TECHNICKÁ OPATŘENÍ

§ 18
Fyzická bezpečnost

Povinná osoba v rámci fyzické bezpečnosti
a) předchází poškození, krádeži nebo zneužití aktiv nebo přerušení poskytování regulované služby,
b) stanoví fyzický bezpečnostní perimetr ohraničující oblast, ve které jsou uchovávány nebo zpracovávány informace a data, nebo ve které jsou umístěna technická aktiva regulované služby,
c) dokumentuje jednotlivé fyzické bezpečnostní perimetry podle písmena b) s ohledem na hodnocení umístěných technických aktiv a rozdělí je na jednotlivé úrovně fyzické ochrany,

d) u každého fyzického bezpečnostního perimetru stanoveného podle písmena c) přijme relevantní bezpečnostní opatření fyzické ochrany s ohledem na jeho úroveň fyzické ochrany
   i) k zamezení neoprávněnému vstupu,
   ii) k zamezení poškození a neoprávněným zásahům,
   iii) k zajištění fyzické ochrany na úrovni objektů a v rámci objektů,
   iv) pro zajištění detekce narušení fyzického bezpečnostního perimetru a
   v) eviduje vstupy a přístupy do fyzického bezpečnostního perimetru.

§ 19
Bezpečnost komunikačních sítí

Povinná osoba pro ochranu bezpečnosti komunikační sítě, a to včetně jejího síťového perimetru
a) zajistí segmentaci komunikační sítě, včetně oddělení provozního, zálohovacího, vývojového, testovacího a jiného specifického prostředí,
b) zajistí řízení komunikace v rámci komunikační sítě,
c) zajistí řízení vzdáleného přístupu ke komunikační síti,
d) zajistí řízení vzdálené správy technických aktiv,
e) v rámci řízení komunikace, vzdáleného přístupu a vzdálené správy povoluje pouze takovou komunikaci, která je nezbytná pro řádné zajištění regulované služby,
f) pomocí kryptografických algoritmů upravených v § 26 zajistí důvěrnost a integritu při přenosu informací a dat v rámci komunikační sítě a
g) využívá nástroj, který zajistí ochranu integrity komunikační sítě.

§ 20
Správa a ověřování identit

1) Povinná osoba používá nástroj pro správu a ověření identity administrátorů, uživatelů a technických aktiv regulované služby.
2) Nástroj pro správu a ověření identity administrátorů, uživatelů a technických aktiv zajišťuje
   a) ověření identity před zahájením jejich aktivit,
   b) řízení počtu možných neúspěšných pokusů o přihlášení,
   c) odolnost uložených a přenášených autentizačních údajů vůči hrozbám a zranitelnostem, které by mohly narušit jejich důvěrnost nebo integritu,
   d) opětovné ověření identity po stanovené době nečinnosti,
   e) dodržení důvěrnosti při vytváření výchozích autentizačních údajů při obnově přístupu a
   f) centralizovanou správu identit s ohledem na vazby mezi aktivy.

3) Povinná osoba pro ověření identity administrátorů, uživatelů a technických aktiv využívá autentizační mechanizmus, který je založený na vícefaktorové autentizaci s nejméně dvěma různými typy faktorů.
4) Povinná osoba do doby splnění požadavků pro ověření identity administrátorů, uživatelů nebo technických aktiv podle odstavce 3 vede evidenci technických aktiv, účtů a autentizačních mechanismů, které tyto požadavky nesplňují, a to včetně odůvodnění.
5) Povinná osoba do doby splnění požadavku pro ověření identity administrátorů, uživatelů nebo technických aktiv využívající autentizační mechanismus založený na vícefaktorové autentizaci s nejméně dvěma různými typy faktorů podle odstavce 3, využívá autentizaci pomocí kryptografických klíčů nebo certifikátů.
6) Povinná osoba do doby splnění požadavku pro ověření identity administrátorů, uživatelů a technických aktiv využívající autentizační mechanismus založený na autentizaci pomocí kryptografických klíčů nebo certifikátů podle odstavce 5, využívá nástroj pro autentizaci pomocí identifikátoru účtu a hesla a tento nástroj musí vynucovat následující pravidla
   a) délky hesla alespoň
      1. 12 znaků pro účty uživatelů,
      2. 17 znaků pro účty administrátorů,
      3. 22 znaků pro účty technických aktiv,
   b) umožňující zadat heslo o délce alespoň 64 znaků,
   c) pro ověření identity technických aktiv musí být výchozí heslo bezodkladně změněno a nové heslo musí být vytvořeno náhodným řetězcem složeným z malých a velkých písmen, číslic a speciálních znaků,
   d) neomezující použití malých a velkých písmen, číslic a speciálních znaků,
   e) umožňující uživatelům a administrátorům změnu hesla, přičemž období mezi dvěma změnami hesla nesmí být kratší než 30 minut,
   f) povinné změny hesla v intervalu maximálně po 18 měsících,
   g) neumožňující uživatelům a administrátorům
      1. zvolit si hesla ze slovníku nejčastěji používaných hesel,
      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.
7) Povinná osoba vytváří náhodné výchozí heslo nebo identifikátor sloužící k vytvoření nebo pro obnovení přístupu v souladu s odstavcem 6.
8) Povinná osoba bezodkladně zneplatní heslo nebo identifikátor sloužící k vytvoření nebo pro obnovení přístupu po jeho prvním použití nebo uplynutím nejvýše 24 hodin od jeho vytvoření.
9) Povinná osoba u administrátorského účtu určeného zejména pro případ obnovy po kybernetickém bezpečnostním incidentu, musí vynucovat následující pravidla
   a) bezodkladně vynutí změnu výchozí hesla,
   b) heslo musí být vytvořeno náhodným řetězcem složeným z malých a velkých písmen, číslic a speciálních znaků,

c) délka hesla musí být alespoň 22 znaků,
d) heslo musí být uloženo na bezpečném místě,
e) s účtem a jeho heslem mohou manipulovat pouze pověřené osoby a to v nezbytně nutných případech,
f) musí být vynucena změna hesla po jeho použití nebo v intervalu maximálně po 18 měsících a
g) eviduje manipulaci a pokusy o manipulaci s tímto účtem a jeho heslem.

§ 21
Řízení přístupových oprávnění

Povinná osoba pro řízení přístupových oprávnění

a) využívá centralizovaný nástroj s ohledem na vazby mezi aktivy,
b) řídí oprávnění pro přístup k jednotlivým aktivům a
c) řídí oprávnění pro čtení dat, zápis dat a změnu oprávnění.

§ 22
Detekce kybernetických bezpečnostních událostí

1) Povinná osoba používá nástroj pro detekci kybernetických bezpečnostních událostí, který v rámci komunikační sítě zajišťuje
   a) ověření a kontrolu přenášených dat v rámci komunikační sítě a mezi komunikačními sítěmi,
   b) ověření a kontrolu přenášených dat na síťovém perimetru komunikační sítě a
   c) blokování nežádoucí komunikace.
2) Povinná osoba používá centrálně spravovaný nástroj s ohledem na vazby mezi aktivy pro detekci kybernetických bezpečnostních událostí, který u jednotlivých relevantních technických aktiv zajišťuje
   a) nepřetržitou a automatickou ochranu před škodlivým kódem,
   b) řízení a sledování používání vyměnitelných zařízení a datových nosičů,
   c) řízení automatického spouštění obsahu vyměnitelných zařízení a datových nosičů,
   d) řízení oprávnění ke spouštění kódu,
   e) řízení a sledování komunikace aplikací, jejich služeb a procesů a
   f) detekci na základě chování technického aktiva, uživatelů a aplikací.
3) Povinná osoba provádí pravidelnou a bezodkladnou aktualizaci nástroje používaného podle odstavce 1 a 2, a to včetně jeho nastavení a detekčních pravidel.

§ 23
Zaznamenávání událostí

1) Povinná osoba na základě hodnocení aktiv a bezpečnostních potřeb určí technická aktiva, u kterých je zaznamenávání bezpečnostních a relevantních provozních událostí prováděno.
2) Povinná osoba v souladu s odstavcem 1 zaznamenává bezpečnostní a relevantní provozní události
   a) detekované podle § 22,
   b) v rámci komunikační sítě,
   c) na síťovém perimetru a
   d) technických aktiv.
3) Povinná osoba aktualizuje rozsah technických aktiv určených podle odstavce 1 v pravidelných intervalech a při významných změnách.
4) Povinná osoba zajišťuje nepřetržitou synchronizaci jednotného času technických aktiv.
5) Povinná osoba v rámci zaznamenávání událostí podle odstavce 2 zaznamenává zejména následující informace o události
   a) datum a čas včetně specifikace časového pásma,
   b) typ činnosti,
   c) jednoznačnou identifikaci technického aktiva, které činnost zaznamenalo,
   d) jednoznačnou identifikaci účtu, pod kterým byla činnost provedena,
   e) jednoznačnou identifikaci zařízení původce a
   f) úspěšnost nebo neúspěšnost činnosti.
6) Povinná osoba zajistí jednoznačnou síťovou identifikaci podle odstavce 5 písm. c), d) a e) v případě, kdy v komunikační síti dochází ke změně této síťové identifikace.
7) Povinná osoba v rámci zajištění důvěrnosti a integrity informací získaných podle odstavce 2 zajistí jejich ochranu před neoprávněným čtením a jakoukoliv změnou.
8) Povinná osoba v rámci zaznamenávání událostí podle odstavce 2, zejména zaznamenává
   a) přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů,
   b) provedení a neúspěšný pokus o provedení privilegované činnosti,
   c) manipulace a neúspěšný pokus o manipulaci s účty, oprávněními a právy,
   d) neprovedení činností v důsledku nedostatku přístupových práv nebo oprávnění,
   e) zahájení a ukončení činností technických aktiv,
   f) kritických a chybových hlášení technických aktiv,
   g) přístup a neúspěšný pokus o přístup k záznamům událostí,
   h) manipulaci a neúspěšný pokus o manipulaci se záznamy událostí,
   i) změnu a neúspěšný pokus o změnu nastavení nástrojů pro zaznamenávání událostí a
   j) další činností uživatelů, které mohou mít vliv na bezpečnost regulované služby.
9) Povinná osoba používá centrální nástroj s ohledem na vazby mezi aktivy pro sběr a uchovávání záznamů událostí zaznamenaných podle odstavce 2.

10) Povinná osoba uchovává záznamy událostí zaznamenané podle odstavce 2 nejméně po dobu 18 měsíců.

§ 24
Vyhodnocování kybernetických bezpečnostních událostí

1) Povinná osoba používá nástroj pro nepřetržité vyhodnocování kybernetických bezpečnostních událostí detekovaných podle § 22 pro
   a) sběr, vyhledávání a seskupování souvisejících záznamů za účelem detekce kybernetických bezpečnostních událostí,
   b) nepřetržité poskytování informací o detekovaných kybernetických bezpečnostních událostech, včasné varování určených bezpečnostních rolí a
   c) vyhodnocování kybernetických bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů.
2) Povinná osoba v rámci používání nástroje v souladu s odstavcem 1 zajistí
   a) omezení případů nesprávného či nežádoucího vyhodnocování kybernetických bezpečnostních událostí,
   b) pravidelnou aktualizaci nastavení nástroje včetně jeho pravidel pro detekci a vyhodnocování kybernetických bezpečnostních událostí a
   c) pravidelnou aktualizaci pravidel pro nepřetržité poskytování informací o detekovaných kybernetických bezpečnostních událostech včetně včasného varování určených bezpečnostních rolí.
3) Povinná osoba využívá informací získaných nástrojem pro vyhodnocení kybernetických bezpečnostních událostí pro optimální nastavení systému řízení bezpečnosti informací regulované služby a zavádění bezpečnostních opatření.

§ 25
Aplikační bezpečnost

1) Povinná osoba pro zajištění bezpečnosti regulované služby užívá technická aktiva, která jsou výrobcem, dodavatelem nebo jinou osobou podporována a zajistí bezodkladné aplikování bezpečnostních aktualizací vydaných pro tato aktiva.
2) Povinná osoba do doby plnění odstavce 1 eviduje technická aktiva, která již nejsou výrobcem, dodavatelem nebo jinou osobou podporována a zavede bezpečnostní opatření, která zaručí obdobnou nebo vyšší úroveň bezpečnosti těchto technických aktiv.
3) Povinná osoba dále v rámci aplikační bezpečnosti zajistí trvalou ochranu aplikací, informací, transakcí a přenášených identifikátorů relací před
   a) neoprávněnou činností a
   b) popřením provedených činností.
4) Povinná osoba provádí pravidelné skenování zranitelnosti technických aktiv regulované služby
   a) z interní a externí komunikační sítě a
   b) alespoň jednou ročně.

5) Povinná osoba zohlední výsledky skenů zranitelnosti v rámci řízení rizik podle § 9 a zavádí bezpečnostní opatření na základě zjištěných výsledků.
6) Povinná osoba provádí penetrační testování technických aktiv s ohledem na hodnocení těchto aktiv a hodnocení rizik
   a) z interní a externí komunikační sítě,
   b) před jejich uvedením do provozu a
   c) v souvislosti s významnou změnou podle § 12 odst. 3.
7) Povinná osoba zohlední výsledky penetračního testování v rámci řízení rizik podle § 9 a zavádí bezpečnostní opatření na základě zjištěných výsledků.
8) Povinná osoba provede opětovné otestování (retest) nálezu zjištěného na základě provedeného skenování zranitelnosti nebo penetračního testování za účelem ověření funkčnosti zavedených bezpečnostních opatření.
9) Povinná osoba v souladu s odstavcem 6 písm. a) provádí pravidelně penetrační testování a to alespoň jednou za dva roky.
10) Povinná osoba v odůvodněných případech, pokud nemůže provést penetrační testování v rozsahu nebo intervalu stanoveném v odstavci 9, může rozdělit toto penetrační testování do systematických celků. V takovém případě je nutno provést penetrační testování v rozsahu stanoveném v odstavci 6 nejpozději do 5 let.

§ 26
Kryptografické algoritmy

1) Povinná osoba pro zajištění ochrany technických aktiv a jejich komunikace
   a) používá aktuálně odolné kryptografické algoritmy,
   b) prosazuje bezpečné nakládání s kryptografickými algoritmy a
   c) zohledňuje doporučení a metodiky v oblasti kryptografických algoritmů vydané Úřadem, zveřejněné na jeho internetových stránkách.
2) Povinná osoba v souladu s odstavcem 1 zajišťuje bezpečnou
   a) hlasovou, audiovizuální a textovou komunikaci, a to včetně e-mailové komunikace a
   b) nouzovou komunikaci v rámci organizace.
3) Povinná osoba v případě využívání kryptografických klíčů a certifikátů pro ochranu technických aktiv a komunikační sítě používá
   a) pouze aktuálně odolné kryptografických klíče a certifikáty a
   b) systém správy klíčů a certifikátů, který
      1. zajistí generování, distribuci, ukládání, změny, omezení platnosti, zneplatnění certifikátů a řádnou likvidaci kryptografických klíčů,
      2. umožní kontrolu a audit a
      3. zajistí důvěrnost a integritu kryptografických klíčů.

§ 27
Zajišťování dostupnosti regulované služby

1) Povinná osoba zavede bezpečnostní opatření pro zajišťování dostupnosti regulované služby, kterými zajistí
   a) dostupnost regulované služby podle cílů stanovených dle § 16,
   b) odolnost regulované služby vůči hrozbám a zranitelnostem, které by mohly snížit její dostupnost a
   c) redundanci aktiv nezbytných pro zajištění dostupnosti regulované služby.
2) Povinná osoba pro zajištění dostupnosti regulované služby v souladu s odstavcem 1 vytváří pravidelné zálohy nastavení technických aktiv, informací a dat nezbytných zejména pro účely obnovy regulované služby pro případ kybernetického bezpečnostního incidentu.
3) Povinná osoba u záloh vytvářených podle odstavce 2 zajistí
   a) pravidelné testování jejich integrity, dostupnosti a obnovitelnosti,
   b) dokumentování výsledků testů provedených podle odstavce 3 písm. a),
   c) ochranu ukládaných záloh a dat v nich obsažených před narušením jejich integrity a důvěrnosti, a to zejména šifrováním těchto záloh v souladu s § 26 a
   d) ochranu ukládaných záloh a dat v nich obsažených před narušením jejich dostupnosti.
4) Povinná osoba za účelem omezení šíření kybernetického bezpečnostního incidentu a snížení jeho dopadu odděluje zálohovací prostředí od jiných prostředí podle § 19 písm. a).

§ 28
Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

Povinná osoba pro zajištění kybernetické bezpečnosti průmyslových, řídicích a obdobných specifických technických aktiv dále využívá nástroje a zavádí bezpečnostní opatření, která zajistí

a) omezení fyzického přístupu k průmyslovým, řídicím a obdobným specifickým technickým aktivům,

b) omezení oprávnění k přístupu k průmyslovým, řídicím a obdobným specifickým technickým aktivům,

c) segmentaci komunikačních sítí průmyslových, řídicích a obdobných specifických technických aktiv od jiných prostředí a segmentaci těchto komunikačních sítí podle § 19,

d) omezení vzdálených přístupů a vzdálené správy průmyslových, řídicích a obdobných specifických technických aktiv,

e) ochranu jednotlivých průmyslových, řídicích a obdobných specifických technických aktiv před využitím známých hrozeb a zranitelností a

f) obnovu dostupnosti průmyslových, řídicích a obdobných specifických technických aktiv.

ČÁST TŘETÍ
LOKALIZACE INFORMACÍ A DAT PŘI ZPRACOVÁNÍ V ZAHRANIČÍ

§ 29
Lokalizace při zpracování dat v zahraničí

1) Povinná osoba posoudí možný dopad kybernetického bezpečnostního incidentu na informace a data zpracovávaná v rámci stanového rozsahu a o tomto posouzení vyhotoví písemný záznam.
2) Povinná osoba v rámci stanoveného rozsahu zajistí, že na území České republiky jsou zpracovávány veškeré informace a data, u nichž kybernetický bezpečnostní incident může
   a) vést ke zranění skupiny více než 2 500 lidí nebo přímému ohrožení nebo ztrátě života skupiny více než 250 lidí,
   b) vést k omezení nebo narušení zpracování osobních údajů, které je nezbytné pro zajišťování obranných a bezpečnostních zájmů České republiky,
   c) vést k závažnému a dlouhodobému narušení schopnosti vyšetřovat trestnou činnost nebo zpochybnění soudního řízení v rámci orgánů činných v trestním řízení,
   d) negativně ovlivnit nebo poškodit diplomatické vztahy České republiky,
   e) vést k finančním ztrátám přesahujícím 10 % běžných výdajů ročního rozpočtu povinné osoby a tyto ztráty odpovídají částce 10 000 000 Kč a vyšší, nebo může způsobit hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu, nebo
   f) způsobit dotčení prvku kritické infrastruktury provozovaného povinnou osobou a může
      1. zapříčinit hromadné nepokoje nebo jinak závažně narušit veřejný pořádek s celostátními dopady,
      2. narušit řádné fungování části nebo celé povinné osoby, přičemž může závažně omezit nebo zastavit provádění důležitých činností povinné osoby a narušit řízení, poškodit rozvoj nebo poškodit prosazování cílů a zájmů povinné osoby,
      3. negativně ovlivnit vztahy s jinými organizacemi nebo vztahy s veřejností a negativní následky mohou být dlouhodobě mezinárodní, nebo
      4. dojít k rozsáhlému omezení poskytování nezbytných služeb nebo jinému závažnému zásahu do každodenního života postihujícího více než 125 000 osob.
3) Povinnost stanovená v odst. 1 se nevztahuje na uchovávání zašifrovaných informací a dat na území členských států Evropské unie, Evropského sdružení volného obchodu, Organizace Severoatlantické smlouvy, Organizace pro ekonomickou spolupráci a rozvoj v případě, že tyto informace a data byly zašifrovány v souladu s § 26 této vyhlášky povinnou osobou.
4) Povinná osoba v rámci stanoveného rozsahu zajistí, že na území členských států Evropské unie, Evropského sdružení volného obchodu, Organizace

Severoatlantické smlouvy nebo Organizace pro ekonomickou spolupráci a rozvoj jsou zpracovávány veškeré informace a data u nichž kybernetický bezpečnostní incident může

a) vést ke zranění skupiny více než 100 lidí a nejvíce 2 500 lidí nebo přímému ohrožení nebo ztrátě života jednotlivce nebo skupiny nejvíce 250 lidí,
b) vést k narušení vyšetřování trestné činnosti nebo soudního řízení v rámci orgánů činných v trestním řízení,
c) zapříčinit hromadné nepokoje nebo jinak závažně narušit veřejný pořádek s regionálními dopady,
d) negativně ovlivnit obraz České republiky ve světě,
e) narušit řádné fungování části nebo celé povinné osoby, přičemž může závažně omezit nebo zastavit provádění důležitých činností povinné osoby a narušit řízení, poškodit rozvoj nebo poškodit prosazování cílů a zájmů povinné osoby,
f) negativně ovlivnit vztahy s jinými částmi povinné osoby, jinými organizacemi nebo vztahy s veřejností, avšak negativní následky mohou být nejvýše celostátní nebo krátkodobě mezinárodní,
g) vést k finančním ztrátám ve výši přesahující 5 % a maximálně 10 % běžných výdajů ročního rozpočtu povinné osoby a tyto ztráty odpovídají částce 1 000 000 Kč a vyšší, nebo může způsobit hospodářské ztráty státu ve výši mezi 0,1 % a 0,5 % hrubého domácího produktu,
h) způsobit omezení, narušení nebo nedostupnost služeb pro více než 50 000 osob, nebo
i) negativně ovlivnit regulovanou službu, která naplňuje dvě a více z níže uvedených kritérií
    1. v rámci regulované služby se zpracovávají zvláštní kategorie osobních údajů nebo údaje vysoce osobní povahy, zejména finanční údaje o stavu majetku, výši finančních prostředků, dluzích nebo půjčkách nebo platební morálce, záznamy o historii soukromých volání subjektů údajů, údaje z \elektronické pošty subjektů údajů a podobně,
    2. v rámci regulované služby dochází ke zpracování osobních údajů, kterým je dotčeno nebo lze důvodně předpokládat, že bude dotčeno více než 10 000 subjektů údajů a
    3. v rámci regulované služby dochází k automatizovanému rozhodování, které se dotýká subjektu údajů.

ČÁST ČTVRTÁ
ZÁVĚREČNÁ USTANOVENÍ

§ 30
Přechodná ustanovení

Poskytovatelé regulované služby, kteří byli ke dni předcházejícímu nabytí účinnosti této vyhlášky orgánem nebo osobou podle § 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti,

kterým se ukládají povinnosti v oblasti zavádění a provádění bezpečnostních opatření podle vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění účinném přede dnem nabytí účinnosti této vyhlášky, a kteří ke dni nabytí účinnosti této vyhlášky naplňují kritéria pro identifikaci alespoň jedné regulované služby, zavádí a provádí v rozsahu stanoveném zákonem o kybernetické bezpečnosti a do doby uplynutí lhůt pro zahájení plnění povinností podle zákona o kybernetické bezpečnosti bezpečnostní opatření podle vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění účinném přede dnem nabytí účinnosti této vyhlášky.

ČÁST PÁTÁ
ÚČINNOST

§ 31
Účinnost

Tato vyhláška nabývá účinnosti dnem dd.mm.rrrr.

Ředitel:
Ing. Lukáš Kintr v. r.

Příloha č. 1 k vyhlášce č. XX/XXXX Sb.

Identifikace a hodnocení aktiv

1) Při identifikaci primárních aktiv regulované služby je vhodné nejprve identifikovat její účel. Z účelu je možné odvodit aktivum typu služba. Následně je vhodné identifikovat s jakými informacemi daná služba pracuje a odvodit primární aktiva typu informace.
2) Při identifikaci podpůrných aktiv je nutné vycházet z architektury systému regulované služby a zejména zohlednit vazby na primární aktiva. Povinná osoba by měla zvolit takový detail podpůrných aktiv, aby byla schopna adekvátně identifikovat a řídit rizika s aktivy spojená.
3) Garanti aktiv jsou určováni na základě jejich pracovního zařazení a procesních a odborných znalostí daného aktiva. Pro účely řízení aktiv musí být garant aktiva schopen na základě možných dopadů aktivum ohodnotit.
4) Pro hodnocení aktiv jsou v tomto případě použity stupnice o čtyřech úrovních uvedené v tabulkách č. 1, 2 a 3 a posuzuje se, jaký dopad by mělo narušení bezpečnosti informací u jednotlivých aktiv. Je doporučeno, aby si povinná osoba tyto hodnotící úrovně aktiv ve stupnici přizpůsobila svým potřebám. Povinná osoba může používat odlišný počet úrovní pro hodnocení aktiv, než jaký je uveden v této příloze, dodrží-li jednoznačné vazby mezi jimi používaným způsobem hodnocení aktiv a stupnicemi a úrovněmi pro hodnocení aktiv, které jsou uvedeny v této příloze.
5) U primárních aktiv je zároveň nutné zohlednit alespoň oblasti uvedené v tabulce č. 4 - Oblasti hodnocení primárních aktiv.
6) Při hodnocení podpůrných aktiv je nutné zohlednit vazby mezi podpůrnými a primárními aktivy. Lze použít např. jednu z následujících variant
   a) podpůrná aktiva přebírají hodnoty primárních aktiv,
   b) podpůrná aktiva jsou posuzována individuálně s ohledem na hodnotu primárních aktiv,
   c) podpůrná aktiva přebírají hodnoty primárních aktiv prostřednictvím vhodně zvoleného vzorce.
7) Pravidla pro ochranu aktiv se vztahují i na listinné dokumenty, vyměnitelná zařízení a datové nosiče, které jsou kopií originálů v elektronické verzi.

Tab. č. 1: Stupnice pro hodnocení důvěrnosti

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy povinné osoby.	Není vyžadována žádná ochrana. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle tzv. traffic light protokolu (dále jen „TLP“) je využíváno označení TLP:CLEAR. Likvidace/mazání aktiva na úrovni Nízká - viz příloha č. 4.
Střední	Aktiva nejsou veřejně přístupná a tvoří know-how povinné osoby, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním.	Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:GREEN nebo TLP:AMBER.

		Likvidace/mazání aktiva na úrovni Střední - viz příloha č. 4.
Vysoká	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (například obchodní tajemství, osobní údaje).	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací komunikačními sítěmi jsou chráněny pomocí kryptografických prostředků. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:AMBER nebo TLP:AMBER+STRICT. Likvidace/mazání aktiva na úrovni Vysoká - viz příloha č. 4.
Kritická	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů).	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Dále metody ochrany zabraňující zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:RED . Likvidace/mazání aktiva na úrovni Kritická - viz příloha č. 4.

Tab. č. 2: Stupnice pro hodnocení integrity

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

	vážnými dopady na primární aktiva.	

Tab. č. 3: Stupnice pro hodnocení dostupnosti

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).	Pro ochranu dostupnosti je postačující pravidelné zálohování.
Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů povinné osoby.	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.
Vysoká	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za velmi důležitá.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.
Kritická	Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za kritická.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.

Tab. 4 Oblasti hodnocení primárních aktiv

Při hodnocení primárních aktiv je potřeba posoudit alespoň relevantní z následujících oblastí

Oblast	Příklad
a) rozsah a důležitost osobních údajů, zvláštních kategorií osobních údajů	Únik osobních údajů fyzické osoby.
b) rozsah dotčených právních povinností nebo jiných závazků nebo obchodního tajemství	Narušení povinnosti zveřejňovat dokumenty na elektronické úřední desce, která musí být nepřetržitě dostupná vzdáleným přístupem. Porušení smlouvy a z ní plynoucí sankce. Únik obchodního tajemství. Porušení legislativy a z toho plynoucí pokuty.
c) rozsah narušení vnitřních řídicích a kontrolních činností	Neúplnost či modifikace informací potřebných pro rozhodování vedení a kontrolní činnost.
d) poškození veřejných, obchodních nebo ekonomických zájmů a možné finanční ztráty	Nedostupnost informací o fakturách na základě nedostupnosti ekonomického systému.

	Nedostupnost informací o možných obchodních příležitostech a z toho plynoucí ušlý zisk. Nedostupnost např. internetových stránek, může vést k neinformování veřejnosti o důležitých skutečnostech (záplavy, ekologické katastrofy atd.).
e) dopady na poskytování důležitých služeb	Narušení všech informací a služeb vztažených směrem k regulované službě a hlavnímu business cíli (účelu existence) organizace.
f) rozsah narušení běžných činností	Narušení činností personálních, ekonomických, správy budov a autoparku, neschopnost přijímat datové zprávy apod.
g) dopady na zachování dobrého jména nebo ochranu dobré pověsti	Nedodržení závazků. Únik interních informací.
h) dopady na bezpečnost a zdraví osob	Neschopnost zajistit základní příjem, potraviny, přístup ke zdravotní péči, svobodu apod. Možnost zranění a ztrát na životech.
i) dopady na mezinárodní vztahy	Únik informací od zahraničních partnerů. Únik informací od partnera, který je součástí mezinárodního koncernu.
j) dopady na uživatele informačního a komunikačního systému	Ztráta možnosti přístupu uživatele ke službě vlivem její nedostupnosti.

Příloha č. 2 k vyhlášce č. XX/XXXX Sb.

Hodnocení rizik

1) Jednoznačné stanovení funkce pro určení rizika je nezbytnou součástí metodiky pro hodnocení rizik podle § 9 této vyhlášky.
2) Hodnota rizika je nejčastěji vyjádřena jako funkce, kterou ovlivňuje hodnota aktiva, hrozba a zranitelnost.
3) Pro hodnocení rizik lze použít například tuto funkci: Riziko = hodnota aktiva × hrozba × zranitelnost.
4) Hodnota aktiva je v tomto případě odvozena z hodnocení aktiv podle přílohy č. 1 této vyhlášky.
5) V případě, že povinná osoba využívá metodu pro hodnocení rizik, která nerozlišuje hodnocení hrozby a zranitelnosti, je možné stupnice pro hodnocení hrozeb a zranitelností sloučit, tzn. vytvořit scénáře kombinující hrozbu a zranitelnost. Sloučení stupnic by nemělo vést ke ztrátě schopnosti rozlišení úrovně hrozby a zranitelnosti. Za tímto účelem lze použít například komentář, který zřetelně vyjádří jak úroveň hrozby, tak i úroveň zranitelnosti. Obdobně se postupuje i v případech, kdy povinná osoba používá jiný počet úrovní pro hodnoty aktiv, hrozeb, zranitelností a rizik.

Tab. č. 1: Stupnice pro hodnocení hrozeb

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

Tab. č. 2: Stupnice pro hodnocení zranitelností

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

	Jsou známé úspěšné pokusy překonání bezpečnostních opatření.

Tab. č. 3: Stupnice pro hodnocení rizik

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

6) Pokud je hodnota rizika vyšší než hranice akceptovatelnosti, je třeba implementovat vhodná bezpečnostní opatření, snížit hodnotu rizika nebo eliminovat riziko a zajistit požadovanou úroveň bezpečnosti informací. Metody pro zvládání rizik jsou následující
   a) akceptace rizika,
   b) redukce a eliminace rizika,
   c) vyhnutí se riziku, nebo
   d) přenesení nebo sdílení rizika.

Příloha č. 3 k vyhlášce č. XXXX Sb.

Zranitelnosti a hrozby

Upozornění: Tato příloha obsahuje jen vybrané kategorie zranitelností a hrozeb. Povinná osoba identifikuje konkrétní hrozby a zranitelnosti podle svých potřeb a specifik. Identifikace konkrétních zranitelností a hrozeb je odpovědností povinné osoby.

Zranitelnosti

1. nedostatečná údržba aktiv,
2. zastaralost aktiv,
3. nedostatečná ochrana perimetru,
4. nedostatečné bezpečnostní povědomí uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholového vedení,
5. nedostatečné zálohování,
6. nevhodné nastavení přístupových oprávnění,
7. nedostatečné postupy a procesy pro detekování kybernetických bezpečnostních událostí a identifikování kybernetických bezpečnostních incidentů,
8. nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit činnost, která může mít vliv na bezpečnost regulované služby
9. nedostatečné stanovení bezpečnostních pravidel a postupů, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholového vedení,
10. nedostatečná ochrana aktiv,
11. nevhodná bezpečnostní architektura
12. nedostatečná míra nezávislé kontroly,
13. neschopnost včasného odhalení pochybení ze strany uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholového vedení,
14. nedostatek zaměstnanců s potřebnou odbornou úrovní znalostí,
15. umístění aktiva mimo fyzickou kontrolu (např. na území cizího státu),
16. umístění aktiva na území státu o jehož právním prostředí nemá povinná osoba dostatečné povědomí,
17. zranitelnosti odhalené při skenování zranitelností a penetračním testování.

Hrozby

1. porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholového vedení,
2. poškození nebo selhání technického anebo programového vybavení,
3. zneužití identity,
4. užívání programového vybavení v rozporu s licenčními podmínkami,
5. škodlivý kód
6. narušení fyzické bezpečnosti,
7. přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie,
8. zneužití nebo neoprávněná modifikace informací,
9. ztráta, odcizení nebo poškození aktiva,

10. nedodržení smluvního závazku ze strany dodavatele,
11. pochybení ze strany uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholového vedení,
12. zneužití vnitřních prostředků, sabotáž,
13. dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb,
14. zaměstnanci s nedostatečnou odbornou úrovní znalostí,
15. cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik,
16. zneužití vyměnitelných technických nosičů dat,
17. napadení elektronické komunikace (odposlech, modifikace),
18. závislost na dodavateli,
19. zneužití státní moci pro přístup k aktivům,
20. zpřístupnění nebo předání aktiv na základě žádosti státu.

Příloha č. 4 k vyhlášce č. XXXX Sb.

Likvidace dat

1) Tato příloha udává povinnosti povinné osoby k definování způsobů likvidace informací a dat a jejich kopií a likvidaci technických aktiv, která jsou nosiči informací a dat s ohledem na úroveň aktiv.
2) Povinná osoba stanoví pravidla pro způsob likvidace informací a dat a jejich kopií a likvidaci technických aktiv, která jsou nosiči informací a dat v souladu s touto přílohou. Tím nejsou dotčeny povinnosti podle jiných právních předpisů. Je nutné zvolit adekvátní úroveň služby nabízející přiměřená bezpečnostní opatření, včetně adekvátních pravidel pro likvidaci informací, dat a technických aktiv, která jsou nosiči informací a dat s ohledem na úroveň aktiv.
3) Pravidla pro likvidaci informací a dat by měla být stanovena přiměřeně úrovni aktiv a měla by zejména zohledňovat
   a) hodnotu aktiva (zejména z pohledu důvěrnosti),
   b) technologii (typy a velikosti nosičů informací a dat),
   c) zda se nosiče informací a dat nachází pod kontrolou organizace či nikoliv,
   d) zda jsou informace a data součástí dedikovaného nebo sdíleného prostředí,
   e) kdo bude likvidaci informací a dat provádět (např. interní zaměstnanec nebo dodavatel),
   f) dostupnost vybavení a nástrojů pro likvidaci,
   g) kapacitu likvidovaných nosičů informací a dat,
   h) zda je k dispozici vyškolený personál,
   i) časovou náročnost likvidace,
   j) cenu likvidace s ohledem na nástroje, školení, validaci a opětovné využití nosiče informací a dat
   k) možné způsoby likvidace informací a dat (například zničením nosiče, několikanásobným přepsáním nosiče informací a dat, znečitelněním, šifrováním a podobně),
   l) použitelné způsoby likvidace informací a dat vzhledem ke stavu nosiče informace (například při poškození zařízení nebude možné použít variantu přepisu dat, ale některý ze způsobů fyzické likvidace).
4) Způsoby likvidace informací a dat a technických aktiv, která jsou nosiči informací a dat a jejich kopií
   i) Odstranění
      1) Způsob likvidace nosičů informací a dat tak, aby byla nedostupná (například odstranění datového souboru, vyhození tištěného dokumentu do odpadu).
      2) Jde o nejméně bezpečný způsob likvidace informací a dat. V případě získání nosiče informací a dat je možné s vynaložením určitého úsilí informace a data obnovit.
      3) Tato metoda není použitelná pro nosiče digitálních informací a dat neumožňující opětovný zápis.

4) Použitelný způsob pro úroveň důvěrnosti aktiva (vychází z přílohy č. 1): nízká.

j) Přepsání

1) Způsob likvidace spočívá v opakovaném přepsání informací a dat nahodilými hodnotami.

2) Jde o středně bezpečný způsob likvidace informací a dat. Volně dostupné nástroje neumožňují obnovení přepsaných informací a dat.

3) Přepsání může být nahrazeno nebo kombinováno bezpečnou likvidací kryptografických klíčů k zašifrované informaci.

4) Tato metoda není vhodná pro poškozená média, média neumožňující opětovný zápis, případně pro média s velkou kapacitou.

5) Použitelný způsob pro úroveň důvěrnosti aktiva (vychází z přílohy č. 1): nízká až kritická.

k) Fyzická likvidace nosiče informací a dat

1) Způsob likvidace spočívající ve zničení nosiče informací a dat, popřípadě v rozebrání zařízení a následném zničení nosiče informací a dat (mechanickým, chemickým či tepelným působením).

2) Jde o nejbezpečnější metodu likvidace informací a dat. Nosič informací a dat po fyzické likvidaci nelze znovu použít pro původní účel. Původní informace a data není možné obnovit ani při vynaložení velkého množství prostředků a úsilí.

3) Použitelný způsob likvidace pro úroveň důvěrnosti aktiva (vychází z přílohy č. 1): střední až kritická.

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

<table>
<tr><td></td><td colspan="4">Přípustný způsob likvidace podle úrovně aktiva</td></tr>
<tr><td>Nosič informace</td><td>1. Nízká</td><td>2. Střední</td><td>3. Vysoká</td><td>4. Kritická</td></tr>
<tr><td rowspan="2">Informace a data na lidsky čitelném nosiči (tištěné dokumenty, poznámky a jiné).</td><td rowspan="2">Odstranění: Vyhození do odpadu.</td><td>Přepsání: Začernění.</td><td colspan="2" rowspan="2">Fyzická likvidace: Znehodnocení nosiče informací a dat použitím skartovacího stroje s podélným i příčným řezem, spálením nebo rozložením.</td></tr>
<tr><td>Fyzická likvidace: Znehodnocení nosiče informací a dat použitím skartovacího stroje.</td></tr>
<tr><td>Mobilní zařízení (mobilní telefony, tablety, notebooky a jiné).</td><td>Odstranění: Vymazání informací a dat, reset zařízení do továrního nastavení.</td><td>Přepsání: Pro zařízení s šifrovaným úložištěm - odstranění informací a dat a reset do továrního nastavení.</td><td colspan="2" rowspan="3">Fyzická likvidace: Rozebrání zařízení a zničení nosiče informací a dat.</td></tr>
<tr><td>Síťová zařízení (router, switch, modem a jiné).</td><td rowspan="2">Odstranění: Vymazání informací a dat, reset do</td><td rowspan="2">Přepsání: Odstranění a zahlcení umělými událostmi (umělý síťový provoz,</td></tr>
<tr><td>Kancelářské vybavení</td></tr>
</table>

<table>
<tr><td>(scanery, tiskárny, fax)</td><td>továrního nastavení.</td><td>testovací tiskové úlohy a podobně.).</td><td colspan="2"></td></tr>
<tr><td rowspan="2">Vnitřní a vnější paměti (magnetické pásky, HDD, SSD, CD, DVD, vyměnitelná média a jiné).</td><td rowspan="2">Odstranění: Smazání informací a dat na úrovni souborového systému.</td><td>Přepsání: Přepsání informací a dat. V případě šifrovaného média je alternativou bezpečná likvidace kryptografických klíčů</td><td colspan="2" rowspan="2">Fyzická likvidace: Zničení nosiče informací a dat.</td></tr>
<tr><td>Fyzická likvidace.</td></tr>
<tr><td rowspan="3">Outsourcing a cloud</td><td colspan="4">Přípustný způsob likvidace informací a dat by měl být stanoven smluvním ujednáním.</td></tr>
<tr><td rowspan="2">Odstranění: Odstranění všech souborů včetně předchozích verzí.</td><td>Přepsání: Použití šifrování datových úložišť na úrovni paměťového média a bezpečná likvidace kryptografických klíčů.</td><td rowspan="2">Přepsání: Použití šifrování datových úložišť na úrovni paměťového média a bezpečná likvidace kryptografických klíčů uložených v certifikovaném hardware security modulu (HSM) řízená zákazníkem (například podle standardu FIPS 140-2 Level 2). Při ukončení služby bude zlikvidován vrchní přístupový klíč a informace a data jsou přepsána.</td><td rowspan="2">Přepsání/fyzická likvidace: Použit způsob viz úroveň “3. Vysoká” nebo použita dedikovaná paměťová kapacita úložiště. Při ukončení služby provedena celková sanitizace všech použitých paměťových médií podle výše uvedených řádků pro úroveň kritická.</td></tr>
<tr><td>Alternativně v případě dedikovaného paměťového média je možné informace a data po ukončení služby přepsat.</td></tr>
</table>

Příloha č. 5 k vyhlášce č. XXXX Sb.

Obsah bezpečnostní politiky a bezpečnostní dokumentace

1. Bezpečnostní politika

1.1. Politika systému řízení bezpečnosti informací

a) Cíle, principy a potřeby systému řízení bezpečnosti informací.

b) Rozsah a hranice systému řízení bezpečnosti informací.

c) Pravidla a postupy pro plánování, řízení a zaznamenávání činnosti lidských a technických zdrojů systému řízení bezpečnosti informací.

d) Pravidla a postupy pro vyhodnocování účinnosti a přezkoumání systému řízení bezpečnosti informací.

e) Pravidla a postupy pro nápravná opatření a zlepšování systému řízení bezpečnosti informací.

1.2. Politika organizační bezpečnosti

a) Určení složení výboru pro řízení kybernetické bezpečnosti a jeho práva a povinnosti.

b) Určení bezpečnostních rolí a jejich práv a povinností.

c) Určení práv a povinností uživatelů a administrátorů.

d) Požadavky na oddělení výkonu činností jednotlivých bezpečnostních rolí.

e) Požadavky na oddělení výkonu bezpečnostních a provozních rolí.

1.3. Politika řízení bezpečnostní politiky a dokumentace

a) Určení osoby odpovědné za pravidelný přezkum a aktualizaci bezpečnostních politik a bezpečnostní dokumentace.

b) Pravidla a postupy pro přezkum a aktualizaci bezpečnostních politik a bezpečnostní dokumentace.

1.4. Politika řízení aktiv

a) Proces řízení aktiv.

b) Odpovědnosti za proces řízení aktiv.

c) Pravidla ochrany jednotlivých úrovní aktiv

1) přípustné způsoby používání aktiv,

2) pravidla pro manipulaci s aktivy,

3) pravidla pro klasifikaci informací,

4) pravidla pro označování aktiv,

5) pravidla správy výměnných médií,

6) pravidla pro bezpečné elektronické sdílení a fyzické přenášení aktiv, a

7) pravidla pro určení způsobu likvidace dat, provozních údajů, informací a jejich kopií nebo likvidaci technických nosičů dat s ohledem na úroveň aktiv.

l) Pravidla a postupy ochrany osobních údajů.

1.5. Politika řízení rizik

a) Proces řízení rizik.

b) Odpovědnosti za proces řízení rizik.

1.6. Politika řízení dodavatelů

a) Pravidla a principy pro výběr dodavatelů.

b) Pravidla pro hodnocení rizik souvisejících s dodavateli.

c) Pravidla a principy určování významných dodavatelů.

d) Náležitosti smlouvy zohledňující relevantní požadavky na dodavatele plynoucí z bezpečnostních politik a bezpečnostní dokumentace.

e) Náležitosti smlouvy o úrovni služeb a způsobu a úrovni realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti.

f) Pravidla pro provádění kontroly zavedení bezpečnostních opatření.

g) Pravidla pro hodnocení dodavatelů.

h) Pravidla pro vedení evidence kontaktních údajů dodavatelů pověřených výkonem systémové a technické podpory.

i) Pravidla pro eliminaci závislosti na jednom dodavateli (zejména problematika vendor lock-in a exit strategie).

1.7. Politika bezpečnosti lidských zdrojů

a) Pravidla a postupy rozvoje bezpečnostního povědomí a způsoby jeho hodnocení

   1) způsoby a formy poučení a školení uživatelů,

   2) způsoby a formy poučení a školení garantů aktiv,

   3) způsoby a formy poučení a školení administrátorů,

   4) způsoby a formy poučení a školení osob zastávajících bezpečnostní role,

   5) způsoby a formy poučení a školení vrcholového vedení

   6) způsoby a formy poučení dodavatelů

b) Bezpečnostní školení nových zaměstnanců.

c) Stanovení lhůt pro pravidelné opakování školení pro uživatele, administrátory, osoby zastávající bezpečnostní role a vrcholové vedení.

d) Pravidla a postupy pro řešení případů porušení bezpečnostní politiky systému řízení bezpečnosti informací.

e) Pravidla a postupy pro ukončení pracovního vztahu nebo změnu pracovní pozice

   1) vrácení svěřených aktiv a odebrání práv při ukončení pracovního vztahu,

   2) změna přístupových oprávnění při změně pracovní pozice.

   3) předání odpovědností při změně pracovní pozice nebo ukončení pracovního vztahu s administrátory nebo osobami zastávajícími bezpečnostní role

f) Pravidla základní kybernetické hygieny.

g) Pravidla pro tvorbu a použití hesel.

h) Pravidla a postupy pro kontrolu dodržování bezpečnostních politik.

i) Způsob vedení přehledu o školeních.

1.8. Politika bezpečného chování uživatelů, administrátorů a osob zastávajících bezpečnostní role

a) Pravidla a postupy pro bezpečné nakládání s technickými aktivy.

b) Pravidla a postupy pro bezpečné nakládání s přístupovými hesly a dalšími autentizačními mechanismy.

c) Pravidla a postupy pro bezpečné použití elektronické pošty a přístupu na internet.

d) Pravidla a postupy pro bezpečný vzdálený přístup.

e) Pravidla a postupy pro bezpečné chování na internetu a sociálních sítích.

f) Pravidla a postupy pro oznamování neobvyklého chování technických aktiv a podezření na jakékoliv zranitelnosti.

1.9. Politika bezpečného používání mobilních zařízení

a) Pravidla a postupy pro bezpečné nakládání a používání mobilních zařízení v interní komunikační síti a mimo ni.

b) Pravidla a postupy pro zajištění bezpečnosti zařízení, která povinná osoba nemá ve své správě (zabezpečení BYOD).

1.10. Politika řízení změn

a) Pravidla a postupy pro řízení změn.

b) Pravidla a postupy pro určování a schvalovaní změn, které mají nebo mohou mít vliv na kybernetickou bezpečnost.

c) Pravidla, postupy a kritéria pro přezkoumávání dopadů změn za účelem určování významných změn.

d) Pravidla a postupy pro hodnocení rizik spojených s významnou změnou a výběru bezpečnostních opatření.

e) Pravidla a postupy pro řízení významných změn.

f) Způsob vedení evidence významných změn.

g) Pravidla a postupy pro testování významných změn před jejich uvedením do provozu, včetně možnosti navrácení do původního stavu (tzv. rollback).

h) Pravidla a postupy pro rozhodování o provedení penetračního testování.

1.11. Politika akvizice, vývoje a údržby

a) Bezpečnostní požadavky pro akvizici, vývoj a údržbu.

b) Bezpečnostní požadavky na oddělení provozního, zálohovacího, vývojového, testovacího a jiných specifických prostředí v rámci akvizice, vývoje a údržby.

c) Bezpečnostní požadavky na vícefaktorovou autentizaci.

d) Bezpečnostní požadavky na kryptografické algoritmy.

e) Bezpečnostní požadavky s ohledem na užití principu nulové důvěry (zero trust).

f) Bezpečnostní požadavky na řízení zranitelností v rámci akvizice, vývoje a údržby.

g) Pravidla a postupy pro nasazení a instalaci technických aktiv.

h) Politika poskytování a nabývání licencí programového vybavení a informací

1) pravidla a postupy nasazení programového vybavení a jeho evidence,

2) pravidla a postupy pro kontrolu dodržování licenčních podmínek.

1.12. Politika řízení přístupu

a) Pravidla a postupy pro práci s nástrojem sloužícím pro správu a ověření identit a nástroje řídící přístupová oprávnění a definování povinností odpovědných osob.

b) Pravidla a postupy pro řízení přístupu a řízení oprávnění včetně užití principů least privilege a need to know.

c) Životní cyklus řízení přístupu a stanovení osob odpovědných za jednotlivé fáze.

d) Životní cyklus řízení oprávnění a stanovení osob odpovědných za jednotlivé fáze.

e) Pravidla a postupy pro řízení privilegovaných a administrátorských oprávnění.

f) Pravidla a postupy pro řízení přístupu pro mimořádné situace

g) Pravidla, postupy a evidence pro účty sloužící zejména pro případ obnovy po kybernetickém bezpečnostním incidentu.

h) Pravidelné přezkoumání přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách.

i) Pravidla, postupy a požadavky na řízení přístupů technických aktiv ve správě a technická aktiva mimo správu povinné osoby.

j) Pravidla pro autentizační mechanismy a politiky hesel.

1.13. Politika zvládání kybernetických bezpečnostních událostí a incidentů

a) Definování kybernetické bezpečnostní události a kybernetického bezpečnostního incidentu.

b) Pravidla a postupy pro nepřetržitou detekci, zaznamenávání a vyhodnocování kybernetických bezpečnostních událostí.

c) Pravidla a postupy pro identifikaci a zvládání kybernetických bezpečnostních incidentů

d) Pravidla a postupy pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu.

e) Pravidla a postupy testování nastavených politik a postupů pro zvládání kybernetických bezpečnostních incidentů.

f) Pravidla a postupy pro oznamování neobvyklého chování technických aktiv a podezření na jakékoliv zranitelnosti.

g) Pravidla a postupy pro vyhodnocení, řešení a určení příčiny řešení kybernetických bezpečnostních incidentů a pro pravidelné aktualizace pravidel pro vyhodnocení kybernetických bezpečnostních událostí.

h) Hlášení kybernetických bezpečnostních incidentů.

i) Evidence kybernetických bezpečnostních incidentů.

1.14. Politika řízení kontinuity činností

a) Práva a povinnosti odpovědných osob.

b) Cíle řízení kontinuity činností pro jednotlivé služby

1) minimální úroveň poskytovaných služeb,

2) doba obnovení chodu,

3) bod obnovení dat.

c) Prioritizace jednotlivých služeb.

d) Způsoby krizové komunikace a hlášení.

e) Komunikační matice s klíčovými osobami pro jednotlivé služby.

f) Eskalační postupy pro krizové situace.

g) Katalog scénářů krizových situací.

h) Postupy pro spuštění a ukončení chodu systému, pro restart nebo obnovení chodu systému po selhání a pro ošetření chybových stavů nebo mimořádných jevů.

i) Způsob a perioda testování jednotlivých plánu kontinuity činností a plánů obnovy.

j) Postupy pro realizaci opatření vydaných Úřadem.

1.15. Politika fyzické bezpečnosti

a) Stanovení fyzických bezpečnostních perimetrů a jejich úrovně.

b) Pravidla a postupy pro ochranu jednotlivých úrovní fyzických bezpečnostních perimetrů.

1) Pravidla a postupy pro kontrolu a evidenci vstupu osob.

2) Pravidla a postupy pro ochranu objektů a umístěných aktiv.

3) Pravidla a postupy pro detekci narušení fyzické bezpečnosti.

1.16. Politika bezpečnosti komunikační sítě

a) Pravidla a postupy pro zajištění segmentace sítě a oddělení jednotlivých prostředí.

b) Pravidla, práva a oprávnění pro jednotlivé segmenty a prostředí s ohledem na povolení pouze nezbytné komunikace.

c) Určení práv a povinností za řízení bezpečného provozu komunikační sítě.

d) Pravidla a postupy pro řízení komunikace v komunikační síti.

e) Pravidla a postupy pro řízení vzdáleného přístupu ke komunikační síti, a to včetně vzdáleného přístupu dodavatelů nebo jiných osob.

f) Pravidla a postupy pro vzdálenou správu technických aktiv, a to včetně vzdálené správy technických aktiv dodavatelem nebo jinými osobami.

1.17. Politika pro zaznamenávání událostí

a) Definování rozsahu, periodicity aktualizace rozsahu technických aktiv a určení osoby odpovědné za aktuálnost tohoto rozsahu.

b) Pravidla a postupy pro napojení technických aktiv na nástroj sloužící pro sběr záznamů o událostech.

c) Pravidla a postupy pro jednoznačnou identifikaci technických aktiv pro jednoznačné určení původce zaznamenané události.

d) Pravidla a postupy sběru, zaznamenávání a uchovávání bezpečnostních a relevantních provozních událostí.

e) Pravidla a postupy pro zaznamenávání činnosti administrátorů, dodavatelů a jiných privilegovaných účtů.

f) Pravidla a postupy pro synchronizaci jednotnéhčasu technických aktiv.

g) Pravidla pro retenci zaznamenaných událostí.

1.18. Politika nasazení, používání a údržby nástrojů pro detekci kybernetických bezpečnostních událostí a nástroje pro sběr a vyhodnocování kybernetických bezpečnostních událostí

a) Pravidla a postupy nasazení nástrojů pro detekci kybernetických bezpečnostních událostí.

b) Postupy a procesy pro detekování kybernetických bezpečnostních událostí ze zaznamenaných událostí.

c) Pravidla, postupy a procesy pro vyhodnocování a reagování na detekované kybernetické bezpečnostní události včetně eskalačních postupů a kontaktů na relevantní osoby.

d) Pravidla a postupy pro optimalizaci nastavení nástrojů určených pro detekci kybernetických bezpečnostních událostí.

e) Pravidla a postupy pro optimální nastavení bezpečnostních vlastností nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí.

f) Opatření pro ochranu přístupu k záznamům o těchto událostech.

1.19. Politika řízení zranitelností a patch management

a) Pravidla a postupy pro omezení instalace programového vybavení.

b) Pravidla a postupy pro zajištění podpory technických aktiv.

c) Pravidla a postupy pro evidenci výrobcem, dodavatelem nebo jinou osobou nepodporovaných technických aktiv.

d) Pravidla a postupy pro práci s aktualizacemi, záplatami a novými verzemi programových prostředků a vybavení a způsob jejich vyhledávání.

e) Pravidla a postupy testování aktualizací, záplat a nových verzí programových prostředků a vybavení.

f) Pravidla a postupy nasazení aktualizací, záplat a nových verzí programových prostředků a vybavení včetně postupů a procesů pro případné nespěšné nasazení a obnovení původního stavu (rollback).

g) Pravidla a postupy pro skenování zranitelností, práci s nálezy a následný opětovné otestování nálezu.

h) Pravidla a postupy pro penetrační testování, práci s nálezy a následný opětovné otestování nálezu.

1.20. Politika používání kryptografie

a) Pravidla a postupy pro používání kryptografických algoritmů zejména v programových prostředcích a vybavení a v rámci komunikační sítě.

b) Pravidla a postupy pro pravidelnou aktualizaci kryptografických algoritmů zejména na základě vydaných doporučení, metodik a bezpečnostních standardů.

c) Pravidla a postupy pro řízení kryptografických klíčů a certifikátů.

d) Pravidla a postupy pro zabezpečení hlasové, audiovizuální, textové (vč. e-mailové) komunikace a nouzové komunikace v rámci organizace.

e) Pravidla a postupy pro šifrování informací a dat.

f) Pravidla a postupy pro šifrování technických aktiv, která jsou nosiči informací a dat (zejména vyměnitelná zařízení, disky, zálohovací média).

1.21. Politika dlouhodobého ukládání, zálohování a obnovy

a) Požadavky na zálohování, obnovu a retenci záloh.

b) Pravidla a postupy pro dlouhodobého ukládání informací a dat.

c) Pravidla a postupy pro zapojení a odebrání technického aktiva v rámci systému zálohování.

d) Pravidla a postupy pro zálohování.

e) Pravidla a postupy pro obnovu záloh.

f) Pravidla a postupy pro kontrolu použitelnosti provedených záloh.

g) Pravidla, postupy a periodicitu pro testování zálohování a obnov.

h) Politika a pravidla pro přístup k zálohám a ukládaným informacím a datům.

2. Obsah bezpečnostní dokumentace

2.1. Plán provádění auditu kybernetické bezpečnosti.

2.2. Zpráva z auditu kybernetické bezpečnosti

a) Cíle auditu kybernetické bezpečnosti.

b) Předmět auditu kybernetické bezpečnosti.

c) Kritéria auditu kybernetické bezpečnosti.

d) Identifikování týmu auditorů a osob, které se auditu kybernetické bezpečnosti zúčastnily.

e) Datum a místo, kde byly prováděny činnosti při auditu kybernetické bezpečnosti.

f) Zjištění z auditu kybernetické bezpečnosti.

g) Závěry auditu kybernetické bezpečnosti.

h) Nápravná opatření pro zajištění souladu s kritérii auditu kybernetické bezpečnosti.

2.3. Zpráva z přezkoumání systému řízení bezpečnosti informací

a) Vyhodnocení bezpečnostních opatření z předchozího přezkoumání systému řízení bezpečnosti informací.

b) Identifikace změn a okolností, které mohou mít vliv na systém řízení bezpečnosti informací.

c) Zpětná vazba o účinnosti řízení bezpečnosti informací

1) neshody a nápravná opatření,

2) výsledky monitorování a měření,

3) výsledky auditu,

4) naplnění cílů systému řízení bezpečnosti informací.

d) Posouzení výsledků hodnocení rizik a stavu plánu zvládání rizik.

m) Posouzení dopadů kybernetických bezpečnostních incidentů na poskytované služby a kybernetickou bezpečnost.

n) Posouzení změn, které mohou mít negativní dopad na systém řízení bezpečnosti informací.

o) Identifikace možností pro neustálé zlepšování.

p) Doporučení potřebných rozhodnutí, stanovení bezpečnostních opatření a osob zajišťujících výkon jednotlivých činností.

2.4. Metodika pro identifikaci a hodnocení aktiv

a) Určení stupnice pro hodnocení primárních aktiv
   1) určení stupnice pro hodnocení úrovní důvěrnosti aktiv,
   2) určení stupnice pro hodnocení úrovní integrity aktiv,
   3) určení stupnice pro hodnocení úrovní dostupnosti aktiv.

b) Určení stupnice pro hodnocení podpůrných aktiv se zohledněním vazeb mezi aktivy.

2.5. Metodika pro identifikaci a hodnocení rizik

a) Určení stupnice pro hodnocení rizik
   1) určení stupnice pro hodnocení hodnoty aktiva,
   2) určení stupnice pro hodnocení úrovní hrozby,
   3) určení stupnice pro hodnocení úrovní zranitelnosti,
   4) určení stupnice pro hodnocení úrovní rizik.

b) Metody a přístupy pro zvládání rizik.

c) Způsoby schvalování akceptovatelných rizik.

2.6. Zpráva o hodnocení aktiv a rizik

a) Shrnutí procesu hodnocení aktiv a rizik.

2.7. Prohlášení o aplikovatelnosti

a) Přehled bezpečnostních opatření požadovaných touto vyhláškou, která nebyla aplikována včetně odůvodnění, proč nebyla aplikována.

b) Přehled aplikovaných bezpečnostních opatření, včetně způsobu jejich realizace.

2.8. Plán zvládání rizik

a) Cíle a přínosy vybraných bezpečnostních opatření pro zvládání jednotlivých rizik včetně vazby na konkrétní rizika.

b) Potřebné zdroje pro jednotlivá bezpečnostní opatření pro zvládání rizik.

c) Osoby zajišťující prosazování jednotlivých bezpečnostních opatření pro zvládání rizik.

d) Termíny zavedení jednotlivých bezpečnostních opatření pro zvládání rizik.

e) Způsob realizace bezpečnostních opatření.

2.9. Plán rozvoje bezpečnostního povědomí

a) Obsah a termíny poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholového vedení.

b) Obsah a termíny vstupních a pravidelných školení.

c) Přehledy, které obsahují předmět jednotlivých školení a seznam osob, které školení absolvovaly.

d) Formy a způsoby hodnocení účinnosti plánu rozvoje bezpečnostního povědomí.

2.10. Přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků

a) Přehled obecně závazných právních předpisů.

b) Přehled vnitřních předpisů a jiných předpisů.

c) Přehled smluvních závazků.

2.11. Metodika pro provedení analýzy dopadů

a) Způsoby hodnocení dopadů kybernetických bezpečnostních incidentů na kontinuitu a posuzování souvisejících rizik.

2.12. Plány kontinuity činností

a) Podmínky aktivace plánu.

b) Specifikace osob, které se mají plánem řídit.

c) Dočasná řešení a postupy pro zajištění kontinuity služby v případě realizace krizového scénáře.

2.13. Plány obnovy

a) Detailní postupy pro obnovení dat včetně pořadí činností, odpovědných osob, potřebného času a zdrojů.

b) Způsob ověření úspěšného obnovení dat ze zálohy.

c) Umístění a popis záloh.

2.14. Evidence technických aktiv, která již nejsou výrobcem, dodavatelem nebo jinou osobou podporována

a) Popis těchto technických aktiv.
b) Garanti těchto technických aktiv.
c) Způsoby zavedení bezpečnostních opatření, která zaručí obdobnou nebo vyšší úroveň bezpečnosti těchto technických aktiv.

2.15. Evidence technických aktiv, účtů a autentizačních mechanismů, které nesplňují požadavek na vícefaktorovou autentizaci

a) Popis těchto technických aktiv, účtů a autentizačních mechanismů
b) Odůvodnění nezavedení vícefaktorové autentizace

2.16. Další doporučená dokumentace

a) Topologie infrastruktury.

b) Segmentace infrastruktury.

c) Přehled technických aktiv v rozsahu systému řízení bezpečnosti informací, zejména síťových zařízení, aktivních prvků, koncových zařízení a serverů,

d) Spojení na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory.

Příloha č. 6 k vyhlášce č. XXXX Sb.

Výbor pro řízení kybernetické bezpečnosti a bezpečnostní role

Tato příloha obsahuje popis doporučených požadavků pro výbor pro řízení kybernetické bezpečnosti a bezpečnostní role uvedené v § 5 a 6.

Tab. č. 1: Výbor pro řízení kybernetické bezpečnosti

Role:	**Výbor pro řízení kybernetické bezpečnosti**
Klíčové činnosti:	a) Odpovědnost za celkové řízení a rozvoj kybernetické bezpečnosti v rámci povinné osoby. b) Tvorba rámce kybernetické bezpečnosti, směrování a zásad kybernetické bezpečnosti povinné osoby (definování strategických cílů a směrování rozvoje v oblasti kybernetické bezpečnosti). c) Definice rolí a odpovědností v rámci systému řízení bezpečnosti informací. d) Definice požadavků na podávání zpráv a kontrolu systému řízení bezpečnosti informací. e) Kontrola aktuálního stavu kybernetické bezpečnosti v rámci povinné osoby a zjišťování, zda dochází k naplňování plánovaných cílů.
Další podmínky:	a) Člen výboru pro řízení kybernetické bezpečnosti musí být alespoň 1. zástupce vrcholového vedení nebo jím pověřená osoba, 2. manažer kybernetické bezpečnosti. b) Členové výboru pro řízení kybernetické bezpečnosti se pravidelně scházejí, přičemž průběh a výstupy z jednání jsou uchovávány v listinné nebo elektronické podobě.

Tab. č. 2: Manažer kybernetické bezpečnosti

Role:	**Manažer kybernetické bezpečnosti**
Klíčové činnosti:	a) Odpovědnost za řízení systému řízení bezpečnosti informací. b) Pravidelný reporting pro vrcholové vedení povinné osoby. c) Pravidelná komunikace s vrcholovým vedením povinné osoby. d) Koordinace a podílení se na procesu řízení aktiv a rizik. e) Předkládání zpráv o hodnocení aktiv a rizik, plánu zvládání rizik a prohlášení o aplikovatelnosti výboru pro řízení kybernetické bezpečnosti. f) Poskytování pokynů pro zajištění bezpečnosti informací při vytváření, hodnocení, výběru, řízení a ukončení dodavatelských vztahů. g) Komunikace s Vládním nebo Národním CERT. h) Koordinace řízení incidentů. i) Vyhodnocování vhodnosti a účinnosti bezpečnostních opatření.
Znalosti:	a) Normy řady ISO/IEC 27000 a obdobné normy z oblasti bezpečnosti a ICT. b) Přehled v oblasti ICT (operační systémy, databáze, aplikace, datové sítě) s důrazem na bezpečnost c) Řízení rizik. d) Řízení kontinuity činností. e) Relevantní právní a regulatorní požadavky, zejména zákon. f) Kontext povinné osoby.
Zkušenosti:	a) Prosazování systému řízení bezpečnosti informací. b) Porozumění definicím rizik a rizikovým scénářům. c) Řízení rizik v rámci povinné osoby. d) Schopnost interpretovat výsledky řízení rizik a koordinovat zvládání rizik.
Vzdělání a praxe:	a) Alespoň 3 roky praxe v oboru informační nebo kybernetické bezpečnosti, nebo

	b) absolvování studia na vysoké škole a alespoň 1 rok praxe v oboru informační nebo kybernetické bezpečnosti.
Relevantní certifikace*:	Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Security Professional (CISSP), Manažer BI (akreditační schéma ČIA).
Další podmínky:	a) Role není slučitelná s rolemi odpovědnými za provoz informačního a komunikačního systému a s dalšími provozními či řídicími rolemi. b) Pro správný výkon této role je zapotřebí zajistit potřebné pravomoci, odpovědnost a rozpočet.

Tab. č. 3: Architekt kybernetické bezpečnosti

Role:	**Architekt kybernetické bezpečnosti**
Klíčové činnosti:	a) Odpovědnost za návrh implementace bezpečnostních opatření. b) Zajišťování architektury bezpečnosti.
Znalosti:	a) Architektura informačních a komunikačních systémů a její navrhování. b) Hardwarové komponenty, nástroje a architektury. c) Operační systémy a software. d) Podnikové procesy a jejich integrace a závislost na ICT. e) Řízení bezpečnosti a rizik. f) Bezpečnost komunikací a sítí. g) Řízení identit a přístupů. h) Hodnocení a testování bezpečnosti. i) Bezpečnost provozu. j) Základní principy bezpečného vývoje softwaru. k) Integrace a závislosti ICT a obchodních procesů.
Zkušenosti:	a) Navrhování implementace bezpečnostních opatření. b) Navrhování architektury bezpečnosti se zaměřením na cíle a bezpečnost. c) Bezpečnost vývoje softwaru.
Vzdělání a praxe:	a) Alespoň 3 roky praxe v oboru informační nebo kybernetické bezpečnosti, nebo b) absolvování studia na vysoké škole a alespoň 1 rok praxe v oboru informační nebo kybernetické bezpečnosti.
Relevantní certifikace*:	Certified Ethical Hacker (CEH), CompTIA Security +, Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Security Professional (CISSP), Manažer BI (akreditační schéma ČIA).
Další podmínky:	Role není slučitelná s rolemi odpovědnými za provoz informačních a komunikačních systémů.

Tab. 4: Auditor kybernetické bezpečnosti

Role:	**Auditor kybernetické bezpečnosti**
Klíčové činnosti:	a) Provádění auditu kybernetické bezpečnosti. b) Hodnocení správnosti a účinnosti zavedených bezpečnostních opatření.
Znalosti:	a) Metodologie a rámce auditu informační bezpečnosti. b) Procesy a postupy interního auditu. c) Role a funkce interního auditu. d) Proces provádění auditu ICT bezpečnosti. e) Strategické a taktické řízení ICT. f) Akvizice, vývoj a nasazení ICT. g) Řízení provozu, údržby a služeb ICT. h) Ochrana aktiv.

	i) Hodnocení kybernetické bezpečnosti, metody testování a vzorkování. j) Relevantní právní předpisy. k) ICT bezpečnost.
Zkušenosti:	a) Plánování auditů informační nebo kybernetické bezpečnosti. b) Provádění auditů kybernetické bezpečnosti nebo auditů systému řízení bezpečnosti informací. c) Analyzování výsledků auditů. d) Psaní auditních závěrů, jejich prezentace a navrhování doporučení vedoucích k nápravě nálezů. e) Reporting stavu plnění zákonných požadavků. f) Provádění auditů se zaměřením na ICT a informační nebo kybernetickou bezpečnost.
Vzdělání a praxe:	a) Alespoň 3 roky praxe v oblasti auditu informační nebo kybernetické bezpečnosti, nebo b) absolvování studia na vysoké škole a alespoň 1 rok praxe v oblasti auditu informační nebo kybernetické bezpečnosti.
Relevantní certifikace*:	Certified Information Systems Auditor (CISA), Certified Internal Auditor (CIA), Certified in Risk and Information Systems Control (CRISC), Lead Auditor Information Security Management Systém (Lead Auditor ISMS), Auditor BI (akreditační schéma ČIA).
Další podmínky:	a) Role není slučitelná s rolemi 1. výboru pro řízení kybernetické bezpečnosti, 2. manažera kybernetické bezpečnosti, 3. architekta kybernetické bezpečnosti, 4. garanta aktiva. b) Role není slučitelná s rolemi odpovědnými za provoz informačních a komunikačních systémů.

Tab. 5: Garant aktiva

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

***** Certifikace může být i jiná než uvedená, jestliže certifikace dokládající odbornou způsobilost bezpečnostních rolí splňuje požadavky ISO 17024.

Příloha č. 7 k vyhlášce č. XXXX Sb.

Řízení dodavatelů - bezpečnostní opatření pro smluvní vztahy

Obsah smlouvy uzavírané s významnými dodavateli:

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

b) ustanovení o oprávnění užívat data,

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

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

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

f) ustanovení o povinnosti dodavatele dodržovat bezpečnostní politiky povinné osoby nebo ustanovení o odsouhlasení bezpečnostních politik dodavatele (nebo odsouhlasení pro dodavatelský vztah relevantních částí bezpečnostních politik) povinnou osobou,

g) ustanovení o řízení změn,

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

i) ustanovení o povinnosti dodavatele informovat povinnou osobu o

   1. kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy,
   2. způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním smlouvy,
   3. významné změně ovládání tohoto dodavatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných tímto dodavatelem k plnění podle smlouvy s povinnou osobou,
   4. žádosti cizozemského orgánu o zpřístupnění nebo předání dat zpracovávaných na území cizího státu, vyjma situace, kdy by takové informování bylo v rozporu s právním řádem v jehož působnosti dochází ke zpracování dat nebo podle kterého byla žádost podána.

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

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

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

m) pravidla pro likvidaci dat,

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

o) ustanovení o sankcích za porušení povinností a

p) ustanovení o zpřístupnění nebo předání dat na základě žádosti cizozemského orgánu o zpřístupnění nebo předání dat zpracovávaných na území cizího státu

1. až po provedení přezkoumání zákonnosti žádosti,
2. až po vynaložení úsilí o zabránění zpřístupnění nebo předání dat v rámci možností daných právním řádem, v jehož působnosti dochází ke zpracování dat nebo podle kterého byla žádost podána,
3. pouze v nezbytném rozsahu.

Příloha č. 8 k vyhlášce č. XXXX Sb.
Doporučená témata pro rozvoj bezpečnostního povědomí

a) Techniky zabezpečení zařízení
b) Zásady zabezpečení uživatelských účtů
c) Používání a správa hesel
d) Ochrana proti nahlížení přes rameno
e) Rizika stahování programů a aplikací
f) Škodlivé programy a jejich projevy
g) Rizika povolení/zakázání spouštění maker
h) Rizika spustitelných souborů
i) Firewall, antivirový program a jejich omezení
j) Aktualizace softwaru
k) Zásady práce v počítačové síti
l) Používání VPN
m) Bezpečnost webových stránek
n) Zálohování, ukládání a šifrování dat
o) Využívání cloudových úložišť
p) Techniky sociálního inženýrství
q) Bezpečná elektronická komunikace
r) Bezpečné používání přenosných technických nosičů dat
s) Základní postup reakce na kybernetickou bezpečnostní událost nebo incident
t) Osobní odpovědnost zaměstnance při dodržování zásad kybernetické bezpečnosti
u) Zásady používání pracovních zařízení pro soukromé účely
v) Zásady používání soukromých zařízení pro pracovní účely
w) Online identita, digitální stopa a její minimalizace