Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

**Manažerské shrnutí**

*Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností (ve své části První a Druhé) 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 nižší.*

*Obsah této vyhlášky je inspirován obsahem současné vyhlášky o kybernetické bezpečnosti, splňuje minimální požadavky kladené obsahem směrnice NIS2 (především čl. 20 a 21), vychází ze zkušeností spojených tvorbou Minimálního bezpečnostního standardu NÚKIB a ve výsledku má za cíl přinést nižší, ale racionální požadavky, bez zbytečných příliš zatěžujících povinností pro organizace.*

*V Části Třetí navazuje na ustanovení v novém Zákoně o kybernetické bezpečnosti, které pro potřeby hlášení kybernetických bezpečnostních incidentů poskytovatelů regulované služby v režimu nižších povinností říká, že si tento poskytovatel má stanovit způsob, jak identifikuje kybernetický bezpečnostní incident s významným dopadem.*

*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 nižších 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 nižších povinností (dále jen „povinná osoba“) upravuje

a) obsah a rozsah bezpečnostních opatření, a

b) způsob stanovení významnosti dopadu kybernetického bezpečnostního incidentu.

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

c) privilegovaným uživatelem orgán či osoba, jejichž činnost na technickém aktivu může mít významný dopad na bezpečnost regulované služby,

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

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

f) zajišťováním minimální úrovně kybernetické bezpečnosti zajištění minimální úrovně kybernetické bezpečnosti aktiv povinné osoby založené na zavedení bezpečnostních opatření.

# ČÁST DRUHÁ
# BEZPEČNOSTNÍ OPATŘENÍ

## § 3

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



[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) 20/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2).

# HLAVA I
# ORGANIZAČNÍ OPATŘENÍ

## § 4
## Zajišťování minimální úrovně kybernetické bezpečnosti

1) Povinná osoba v rámci zajišťování minimální úrovně kybernetické bezpečnosti
   a) stanoví strategické cíle zajišťování minimální úrovně kybernetické bezpečnosti,
   b) na základě strategických cílů zajišťování minimální úrovně kybernetické bezpečnosti a bezpečnostních potřeb zavede bezpečnostní opatření směřující k zajištění bezpečnosti regulované služby,
   c) vytvoří a schválí bezpečnostní politiku v oblasti zajišťování minimální úrovně kybernetické bezpečnosti, která obsahuje hlavní zásady, strategické cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení kybernetické bezpečnosti, a na základě bezpečnostních potřeb stanoví bezpečnostní politiku a bezpečnostní dokumentaci v dalších oblastech podle § 7,
   d) zajistí pravidelné vyhodnocení účinnosti zajišťování minimální úrovně kybernetické bezpečnosti, které obsahuje
      i) vyhodnocení strategických cílů zajišťování minimální úrovně kybernetické bezpečnosti stanovených podle písmena a),
      ii) posouzení naplňování plánu zavádění bezpečnostních opatření zpracovaného podle odstavce 2 písm. a),
      iii) posouzení výsledků kontrol provedených v oblasti kybernetické bezpečnosti,
      iv) výsledky předchozích vyhodnocení účinnosti zajišťování minimální úrovně kybernetické bezpečnosti provedených podle písmene d),
      v) posouzení dopadů kybernetických bezpečnostních incidentů s významným dopadem na poskytované služby podle § 13,
      vi) posouzení změn, které mohou mít negativní dopad na zajišťování minimální úrovně kybernetické bezpečnosti podle § 11,
   e) na základě vyhodnocení účinnosti zajišťování minimální úrovně kybernetické bezpečnosti podle písmene d) zpracuje zprávu o přezkoumání zajišťování minimální úrovně kybernetické bezpečnosti,
   f) aktualizuje zajišťování minimální úrovně kybernetické bezpečnosti a příslušnou dokumentaci na základě
      i) zjištění z kontrol provedených v oblasti kybernetické bezpečnosti,
      ii) výsledků vyhodnocení účinnosti zajišťování minimální úrovně kybernetické bezpečnosti, a
      iii) dopadů kybernetických bezpečnostních incidentů s významným dopadem na poskytované služby,
   g) stanoví proces řízení výjimek z pravidel stanovených podle písmene c).
2) Povinná osoba v rámci zajišťování minimální úrovně kybernetické bezpečnosti dále
   a) zpracuje plán zavádění bezpečnostních opatření, který obsahuje

i) popis bezpečnostních opatření,
ii) určení osoby odpovědné za zavedení jednotlivých bezpečnostních opatření,
iii) potřebné lidské, finanční a technické zdroje pro zavedení bezpečnostních opatření,
iv) požadovaný termín zavedení bezpečnostních opatření.

b) zpracuje přehled bezpečnostních opatření, který obsahuje přehled všech bezpečnostních opatření požadovaných touto vyhláškou, která
i) nebyla aplikována, včetně odůvodnění a přehledu přijatých náhradních bezpečnostních opatření,
ii) byla aplikována, včetně způsobu plnění.

3) Povinná osoba v souladu se strategickými cíli zajišťování minimální úrovně kybernetické bezpečnosti stanovenými podle odstavce 1 písm. a) a s plánem zavádění bezpečnostních opatření zavádí bezpečnostní opatření.

## § 5
## Povinnosti vrcholového vedení

1) Vrcholové vedení povinné osoby s ohledem na zajišťování minimální úrovně kybernetické bezpečnosti
a) se prokazatelně účastní školení podle § 10 odst. 2 písm. a),
b) zajistí stanovení bezpečnostní politiky a strategických cílů zajišťování minimální úrovně kybernetické bezpečnosti,
c) zajistí dostupnost zdrojů potřebných pro zajišťování minimální úrovně kybernetické bezpečnosti v souladu s plánem zavádění bezpečnostních opatření,
d) informuje zaměstnance o významu zajišťování minimální úrovně kybernetické bezpečnosti a významu dosažení shody s jeho požadavky se všemi dotčenými stranami,
e) zajistí podporu k dosažení zamýšlených strategických cílů,
f) se podílí na vypracování analýzy dopadů podle § 14,
g) prosazuje neustálé zlepšování zajišťování minimální úrovně kybernetické bezpečnosti,
h) určí osoby zastávající bezpečnostní role a stanoví příslušné pravomoci,
i) podporuje bezpečnostní role v oblastech její odpovědnosti,
j) přijímá bezpečnostní opatření vedoucí
i) ke kontinuálnímu zlepšování zajišťování minimální úrovně kybernetické bezpečnosti a
ii) k dosažení stanovených strategických cílů v oblasti kybernetické bezpečnosti.

2) Vrcholové vedení se prokazatelně seznamuje
a) se zprávou o přezkoumání zajišťování minimální úrovně kybernetické bezpečnosti,
b) s výsledky analýzy dopadů v souladu s § 14,
c) s výsledky kontrol provedených v oblasti kybernetické bezpečnosti.

3) Vrcholové vedení v rámci zajišťování minimální úrovně kybernetické bezpečnosti určí osobu, která bude zastávat bezpečnostní roli
   a) odpovědnou za kybernetickou bezpečnost včetně stanovení jejích povinností, odpovědností a pravomocí a
   b) garanta aktiva.
4) Vrcholové vedení zajistí zastupitelnost osoby odpovědné za kybernetickou bezpečnost.

## § 6
## Bezpečnostní role

1) Osoba odpovědná za kybernetickou bezpečnost odpovídá za řízení a rozvoj kybernetické bezpečnosti, dohled nad stavem kybernetické bezpečnosti, za naplňování plánu zavádění bezpečnostních opatření a komunikaci v oblasti kybernetické bezpečnosti s vrcholovým vedením, přičemž výkonem této role může být pověřena osoba, která pro tuto činnost
   a) bez zbytečného odkladu absolvuje odborné školení podle § 10 odst. 2 písm. e) nebo
   b) prokáže odbornou způsobilost v oblasti kybernetické bezpečnosti.
2) Garant aktiva je bezpečnostní role odpovědná za zajištění rozvoje, použití a bezpečnost aktiva.

## § 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. 3 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 a 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 alespoň v rozsahu uvedeném v příloze č. 1 k této vyhlášce, včetně stanovení úrovní aktiv,

b) určí a eviduje garanty aktiv,

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

d) v rámci hodnocení primárních aktiv posuzuje relevantní 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,

g) pro jednotlivé úrovně primárních aktiv podle písmene a) stanovuje a zavádí pravidla ochrany nutná pro zabezpečení jejich důvěrnosti, dostupnosti a integrity, které obsahují zejména přípustné způsoby používání aktiv,

   i) pravidla pro manipulaci s aktivy,

   ii) pravidla pro klasifikaci informací,

   iii) pravidla pro označování aktiv,

   iv) pravidla správy výměnných médií,

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

   vi) pravidla pro určení způsobu likvidace informací a dat a jejich kopií a likvidace technických aktiv, která jsou nosiči informací a dat s ohledem na úroveň aktiv v souladu s přílohou č. 2 k této vyhlášce.

## § 9
## Řízení dodavatelů

1) Povinná osoba při uzavírání smlouvy s dodavateli související se správou nebo dodávkou technických aktiv, která jsou podle hodnocení těchto aktiv významná pro regulovanou službu

   a) stanoví přiměřená pravidla zohledňující požadavky zajišťování minimální úrovně kybernetické bezpečnosti pro tyto dodavatele na základě zjištěných bezpečnostních potřeb a pravidelně tato pravidla aktualizuje,

   b) seznamuje tyto dodavatele s pravidly podle písmene a) a vyžaduje plnění těchto pravidel,

   c) identifikuje a eviduje tyto dodavatele,

d) s ohledem na určené strategické cíle zajišťování minimální úrovně kybernetické bezpečnosti a zjištěné bezpečnostní potřeby zohledňuje přiměřená bezpečnostní opatření při uzavíraní smluv s těmito dodavateli,
e) zajistí, aby smlouvy s těmito dodavateli obsahovaly zejména relevantní oblasti uvedené v příloze č. 4 k této vyhlášce a

2) Povinná osoba u dodavatelů podle odstavce 1.
a) provádí pravidelné vyhodnocení a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných plnění pomocí vlastních zdrojů nebo pomocí třetí strany a
b) zajistí řešení nedostatků zjištěných podle písmene a).

## § 10
## Bezpečnost lidských zdrojů

1) Povinná osoba v rámci řízení bezpečnosti lidských zdrojů s ohledem na stav a potřeby zajišťování minimální úrovně kybernetické bezpečnosti 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 a o bezpečnostní politice zejména v oblasti zajišťování minimální úrovně kybernetické bezpečnosti, a to
i) bez zbytečného odkladu a
ii) v pravidelných intervalech,
b) poučení uživatelů a administrátorů o jejich povinnostech a o bezpečnostní politice, a to
i) bez zbytečného odkladu a
ii) v pravidelných intervalech,
c) poučení osob zastávajících bezpečnostní role o jejich povinnostech a o bezpečnostní politice, a to
i) bez zbytečného odkladu po jejich pověření výkonem dané bezpečnostní role a
ii) v pravidelných intervalech,
d) poučení relevantních zaměstnanců dodavatelů o jejich povinnostech a o bezpečnostní politice, a to
i) bez zbytečného odkladu po uzavření smluvního vztahu a
ii) pravidelně v průběhu jeho trvání,
e) potřebná odborná teoretická i praktická školení administrátorů a osob zastávajících bezpečnostní role v souladu s jejich pracování náplní,
f) pravidla tvorby bezpečných hesel v souladu s § 17,
g) relevantní témata uvedená v příloze č. 6 této vyhlášky.

3) Povinná osoba v rámci řízení bezpečnosti lidských zdrojů dále
a) zajistí zvyšování bezpečnostního povědomí v souladu s plánem rozvoje bezpečnostního povědomí,

b) zajistí kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostních role a
c) určí pravidla a postupy pro řešení případů porušení stanovených pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.

4) Povinná osoba vede o poučení a školení podle odstavce 2 přehledy, které obsahují předmět poučení a školení včetně seznamu osob, které poučení a školení absolvovaly.

## § 11
## Řízení změn, akvizice, vývoje a údržby

1) Povinná osoba v rámci řízení změn, které mohou mít negativní dopad na důvěrnost, integritu a dostupnost regulované služby
   a) eviduje tyto změny,
   b) dokumentuje řízení těchto změn,
   c) přijímá bezpečnostní opatření za účelem snížení všech nepříznivých dopadů těchto změn a
   d) aktualizuje bezpečnostní a provozní dokumentaci.
2) Povinná osoba v souvislosti s plánovanou akvizicí, vývojem a údržbou aktiv
   a) stanoví bezpečnostní požadavky v oblasti kybernetické bezpečnosti,
   b) při stanovení bezpečnostních požadavků vychází zejména z
      i) požadavků na bezpečnostní opatření podle této vyhlášky,
      ii) informací uvedených v přehledu bezpečnostních opatření zpracovaném podle § 4 odst. 2 písm. b) a
      iii) specifických potřeb organizace,
   c) dodržuje a vymáhá dodržování požadavků stanovených podle odstavce 2 písm. a).

## § 12
## Řízení přístupu

1) Povinná osoba na základě provozních a bezpečnostních 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 § 17 a § 18.
2) Povinná osoba dále v rámci řízení přístupu k aktivům
   a) přidělí každému uživateli a administrátorovi přistupujícímu k technickým aktivům přístupová práva a oprávnění a jedinečný identifikátor,
   b) řídí identifikátory, přístupová práva a oprávnění účtů technických aktiv,
   c) zavádí bezpečnostní opatření pro řízení přístupu technických aktiv k jiným aktivům,
   d) 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,

e) omezí přidělování administrátorských a privilegovaných oprávnění na úroveň nezbytně nutnou k výkonu náplně práce,
f) omezí a kontroluje používání programových prostředků a vybavení, které mohou být schopné překonat systémové nebo aplikační kontroly,
g) prosazuje, aby byly při používání privátních autentizačních informací a mechanismů dodržována stanovená pravidla a postupy,
h) přiděluje a odebírá přístupová oprávnění v souladu s politikou řízení přístupu,
i) provádí pravidelné přezkoumání nastavení veškerých přístupových oprávnění,
j) zajistí odebrání nebo změnu přístupových oprávnění při změně pozice nebo zařazení uživatelů nebo administrátorů,
k) zajistí odebrání nebo změnu přístupových oprávnění při ukončení nebo změně smluvního vztahu,
l) dokumentuje přidělování a odebírání přístupových oprávnění a
m) využívá nástroj pro správu a ověřování identity podle § 17 a nástroj pro řízení přístupových oprávnění podle § 18.

## § 13
## 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 posuzování kybernetických bezpečnostních událostí v souladu s § 19 a § 20 a zvládání kybernetických bezpečnostních incidentů,
   b) přidělí odpovědnosti pro
      i) detekci, zaznamenávání a posuzování kybernetických bezpečnostních událostí a
      ii) koordinaci a zvládání kybernetických bezpečnostních incidentů,
   c) zajistí, že uživatelé, administrátoři, osoby zastávající bezpečnostní role, další zaměstnanci a dodavatelé budou oznamovat neobvyklé chování technických aktiv a podezření na jakékoliv zranitelnosti,
   d) vytvoří metodiku pro posuzování kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů, včetně těch s významným dopadem v souladu s § 25,
   e) zajistí posuzování kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů, včetně těch s významným dopadem v souladu s metodikou podle písmene d),
   f) zajistí zvládání kybernetických bezpečnostních incidentů podle stanovených postupů,
   g) přijímá bezpečnostní opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu,

h) hlásí kybernetické bezpečnostní incidenty s významným dopadem podle zákona,
i) vede záznamy o kybernetických bezpečnostních incidentech a o jejich zvládání,
j) prošetří a určí příčiny kybernetického bezpečnostního incidentu s významným dopadem a
k) vyhodnotí účinnost řešení kybernetického bezpečnostního incidentu s významným dopadem a na základě vyhodnocení stanoví nutná bezpečnostní opatření, popřípadě aktualizuje stávající bezpečnostní opatření k zamezení opakování řešeného kybernetického bezpečnostního incidentu.

2) Povinná osoba zajistí detekci kybernetických bezpečnostních událostí a dále při jejich detekci používá nástroje podle § 19.

### § 14
### Řízení kontinuity činností

1) 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,
c) stanoví práva a povinnosti administrátorů a osob zodpovědných za kybernetickou bezpečnost podílejících se na zajištění poskytování regulované služby,
d) na základě výsledků analýzy dopadů dle písmene b) vypracuje, aktualizuje a testuje plány kontinuity činností a plány obnovy související s poskytováním regulované služby,
e) stanoví pravidla a postupy k provádění pravidelného zálohování,
f) stanoví pravidla a postupy kontroly použitelnosti provedených záloh,
g) provádí pravidelné zálohování a kontrolu použitelnosti záloh podle § 23 a
h) realizuje bezpečnostní opatření pro zvýšení odolnosti podle § 23.

2) Povinná osoba při tvorbě plánů kontinuity činností může využít vzor z přílohy č. 5 k této vyhlášce.

## HLAVA II
## TECHNICKÁ OPATŘENÍ

### § 15
### 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) u fyzického bezpečnostního perimetru přijme relevantní bezpečnostní opatření 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 a

   iv) pro zajištění detekce narušení fyzického bezpečnostního perimetru.

## § 16
## 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 § 22 zajistí důvěrnost a integritu při přenosu informací a dat v rámci komunikační sítě a

g) zajistí ochranu integrity komunikační sítě.

## § 17
## 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 mechanismus, který je založený na vícefaktorové autentizaci s nejméně dvěma různými typy faktorů.
4) 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.
5) 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 4, využívá nástroj pro autentizaci pomocí identifikátoru účtu a hesla a tento nástroj musí vynucovat následující pravidla
   a) délky hesla alespoň
      i) 12 znaků pro účty uživatelů,
      ii) 17 znaků pro účty administrátorů,
      iii) 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
      i) zvolit si hesla ze slovníku nejčastěji používaných hesel,
      ii) tvořit hesla na základě mnohonásobně opakujících se znaků, přihlašovacího jména, e-mailu, názvu systému nebo obdobným způsobem a
      iii) opětovné použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel.
6) Povinná osoba vytváří náhodné výchozí heslo nebo identifikátor sloužící k vytvoření nebo pro obnovení přístupu v souladu s odstavcem 5.
7) 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.
8) 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,
g) eviduje manipulaci a pokusy o manipulaci s tímto účtem a jeho heslem.

## § 18
## 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.

## § 19
## 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 nástroj 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,
   f) detekci na základě chování technického aktiva, uživatelů a aplikací a
   g) nepřetržité poskytování informací o detekovaných kybernetických bezpečnostních událostech a včasné varování určených osob.
3) Povinná osoba provádí pravidelnou a bezodkladnou aktualizaci nástroje používaného podle odstavce 1 a 2, a to včetně jeho nastavení a detekčních pravidel.

## § 20
## Zaznamenávání událostí

1) Povinná osoba na základě hodnocení aktiv a bezpečnostních požadavků 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 § 19,
b) v rámci komunikační sítě,
c) na síťovém perimetru a
d) technických aktiv.

3) Povinná osoba provádí pravidelný přezkum za účelem určení technických aktiv podle odstavce 1.
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) manipulaci 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) kritická a chybová 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 činnosti uživatelů, které mohou mít vliv na bezpečnost regulované služby.
9) Povinná osoba používá nástroj pro sběr a uchovávání záznamů událostí zaznamenaných podle odstavce 2.
10) Povinná osoba uchovává záznamy událostí zaznamenané podle odstavce 2 nejméně po dobu 12 měsíců.

**§ 21**

**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 požadavku podle 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 skenování zranitelnosti v rámci zajišťování minimální úrovně kybernetické bezpečnosti a zavádí bezpečnostní opatření na základě zjištěných výsledků.
6) Povinná osoba v odůvodněných případech, pokud nemůže provést skenování zranitelnosti podle odstavce 4, může rozdělit skenování zranitelností do systematických celků. V takovém případě je nutno provést skenování zranitelnosti v rozsahu podle odstavce 4 nejpozději do 2 let.
7) Povinná osoba přiměřeně provádí penetrační testování technických aktiv, která jsou podle hodnocení těchto aktiv významná pro regulovanou službu,
   a) z interní a externí komunikační sítě a
   b) před jejich uvedením do provozu.
8) Povinná osoba zohlední výsledky penetračního testování v rámci zajišťování minimální úrovně kybernetické bezpečnosti a zavádí bezpečnostní opatření na základě zjištěných výsledků.

## § 22
## 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 kryptografické klíče a certifikáty a
   b) systém správy klíčů a certifikátů, který
      i) zajistí generování, distribuci, ukládání, změny, omezení platnosti, zneplatnění certifikátů a řádnou likvidaci kryptografických klíčů,
      ii) umožní kontrolu a audit a

iii) zajistí důvěrnost a integritu kryptografických klíčů.

## § 23
## Zajišťování dostupnosti regulované služby

1) Povinná osoba zavede bezpečnostní opatření pro zajišťování dostupnosti regulované služby, kterými zajistí
   a) dostupnost regulované služby s ohledem na hodnocení aktiv,
   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 důvěrnosti a integrity, a to zejména šifrováním těchto záloh v souladu s § 22 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 § 16 písm. a).

## § 24
## 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 § 16,

d) omezení vzdáleného přístupu 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
## ZPŮSOB STANOVENÍ VÝZNAMNOSTI KYBERNETICKÉHO BEZPEČNOSTNÍHO INCIDENTU

### § 25
### Stanovení významnosti dopadu kybernetického bezpečnostního incidentu

1) Povinná osoba pro potřeby vyhodnocení významnosti dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby stanoví
   a) únosnou míru újmy způsobené kybernetickým bezpečnostním incidentem představující úhrn nejvyšší škody a nemajetkové újmy vzniklý v souvislosti s kybernetickým bezpečnostním incidentem, v jehož důsledku ještě nejsou ohroženy život či zdraví osob nebo schopnost poskytovatele regulované služby dostát svým závazkům,
   b) oblasti pro posouzení významnosti dopadu kybernetických bezpečnostních incidentů na organizaci zohledňující
      i) provozní dopad kybernetického bezpečnostního incidentu na povinnou osobu a jeho schopnost poskytovat regulovanou službu,
      ii) množství zaměstnanců, uživatelů regulované služby a jiných orgánů a osob zasažených kybernetickým bezpečnostním incidentem,
      iii) čas a zdroje potřebné k obnově poskytování zasažené regulované služby,
      iv) lokaci incidentu vymezující významnost části aktiv zasažených kybernetickým bezpečnostním incidentem pro poskytování regulované služby,
      v) citlivost dat zasažených kybernetickým bezpečnostním incidentem a škodu či nemajetkovou újmu, jakou může porušení zabezpečení těchto dat způsobit povinné osobě či jinému orgánu nebo osobě,
      vi) příčinu kybernetického bezpečnostního incidentu, je-li povinné osobě známa, a to zejména zda byla přímou příčinou lidská chyba, technická závada, nebo úmysl.
2) Dopad kybernetického bezpečnostního incidentu na poskytování regulované služby je považován za významný, pokud přesáhne povinnou osobou stanovenou únosnou míru újmy způsobené kybernetickým bezpečnostním incidentem podle odstavce 1 písm. a), a zároveň je na základě oblastí podle odstavce 1 písm. b) posouzen jako významný.

## ČÁST ČTVRTÁ
## ÚČINNOST

### § 26
### 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.
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.<br>V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle tzv. traffic light protokolu (dále jen „TLP“) je využíváno označení TLP:CLEAR.<br>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.<br>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.<br>V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:AMBER nebo TLP:AMBER+STRICT.<br>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.<br>V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:RED .<br>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.<br>Porušení smlouvy a z ní plynoucí sankce.<br>Únik obchodního tajemství.<br>Porušení legislativy a z toho plynoucí sankce. |
| 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.<br>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.<br>Únik interních informací. |
| h) dopady na bezpečnost a zdraví osob | Neschopnost zajistit základní příjem, potraviny, přístup ke zdravotní péči, svobodu apod.<br>Možnost zranění a ztrát na životech. |
| i) dopady na mezinárodní vztahy | Únik informací od zahraničních partnerů.<br>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.**
**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) a
   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, jsou:
   a) 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.

b) 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.

c) 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 k této vyhlášce)**

<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="2">Fyzická likvidace: Rozebrání zařízení a zničení nosiče informací a dat.</td></tr>
<tr><td>Síťová zařízení (router, switch, modem a jiné).</td><td>Odstranění: Vymazání informací a</td><td>Přepsání: Odstranění a zahlcení umělými</td></tr>
</table>

<table>
<tr><td>Kancelářské vybavení (scanery, tiskárny, fax)</td><td>dat, reset do továrního nastavení.</td><td>událostmi (umělý síťový provoz, 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="2">Outsourcing a cloud</td><td colspan="4">Přípustný způsob likvidace informací a dat by měl být stanoven smluvním ujednáním.</td></tr>
<tr><td>Odstranění: Odstranění všech souborů včetně předchozích verzí.</td><td>Přepsání: Použití šifrování datových úložišť na úrovni paměťového média a bezpečná likvidace kryptografických klíčů.</td><td>Přepsání: Použití šifrování datových úložišť na úrovni paměťového média a bezpečná likvidace kryptografických klíčů uložených v certifikovaném hardware security modulu (HSM) řízená zákazníkem (například podle standardu FIPS 140-2 Level 2). Při ukončení služby bude zlikvidován vrchní přístupový klíč a informace a data jsou přepsána.</td><td>Přepsání/fyzická likvidace: Použit způsob viz úroveň “3. Vysoká” nebo použita dedikovaná paměťová kapacita úložiště. Při ukončení služby provedena celková sanitizace všech použitých paměťových médií podle výše uvedených řádků pro úroveň kritická.</td></tr>
</table>

**Příloha č. 3 k vyhlášce č. XX/XXXX Sb.**

**Bezpečnostní politika a bezpečnostní dokumentace**

1. Bezpečnostní politika

1.1. Politika zajišťování minimální úrovně kybernetické bezpečnosti

a) Strategické cíle, principy a potřeby zajišťování minimální úrovně kybernetické bezpečnosti.
b) Rozsah a hranice řízení kybernetické bezpečnosti.
c) Pravidla a postupy pro vyhodnocování účinnosti zajišťování minimální úrovně kybernetické bezpečnosti.
d) Pravidla a postupy pro nápravná opatření a zlepšování zajišťování minimální úrovně kybernetické bezpečnosti.

1.2. Politika organizační bezpečnosti

a) Určení bezpečnostních rolí a jejich práv a povinností.
b) Určení práv a povinností uživatelů a administrátorů.

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.

1.5. Politika řízení dodavatelů

a) Pravidla a principy pro výběr dodavatelů aktiv významných pro regulovanou službu.
b) Náležitosti smlouvy zohledňující relevantní požadavky na dodavatele plynoucí z bezpečnostních politik a bezpečnostní dokumentace.
c) Náležitosti smlouvy o úrovni služeb a způsobu a úrovni realizace bezpečnostních opatření.
d) Pravidla pro provádění pravidelného přezkoumání plnění smluv s dodavateli z hlediska zajišťování minimální úrovně kybernetické bezpečnosti.
e) Pravidla pro vedení evidence kontaktních údajů dodavatelů pověřených výkonem systémové a technické podpory.

1.7. Politika bezpečnosti lidských zdrojů

a) Pravidla 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 pro řešení případů porušení bezpečnostní politiky.
e) Pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice
1) vrácení svěřených aktiv a odebrání práv při ukončení pracovního vztahu,
2) změna přístupových oprávnění při změně pracovní pozice,
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 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 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, akvizice, vývoje a údržby
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) Způsob vedení evidence a dokumentace změn.
d) Bezpečnostní požadavky pro akvizici, vývoj a údržbu, jako např:
1) Bezpečnostní požadavky na vícefaktorovou autentizaci.
2) Bezpečnostní požadavky na kryptografické algoritmy.
3) Bezpečnostní požadavky s ohledem na užití principu nulové důvěry (zero trust).
4) Bezpečnostní požadavky na řízení zranitelností v rámci akvizice, vývoje a údržby.
e) Pravidla a postupy pro nasazení a instalaci technických aktiv.

1.11. 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 přístupů 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.

1.12. 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 posuzování kybernetických bezpečnostních událostí.
c) Pravidla a postupy pro koordinaci a zvládání kybernetických bezpečnostních incidentů.
d) Pravidla a postupy pro identifikaci a klasifikaci incidentů s významným dopadem
   1) Stanovení únosné míry újmy způsobené kybernetickým bezpečnostním incidentem.
   2) Stanovení oblastí pro posouzení významnosti dopadu kybernetických bezpečnostních incidentů.
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, prošetření a určení příčiny kybernetických bezpečnostních incidentů s významným dopadem a pro pravidelné aktualizace pravidel pro vyhodnocení kybernetických bezpečnostních událostí.
h) Hlášení kybernetických bezpečnostních incidentů.
i) Evidence kybernetických bezpečnostních incidentů.

1.13. Politika řízení kontinuity činností
a) Práva a povinnosti odpovědných osob.
b) Prioritizace jednotlivých služeb.
c) Způsoby krizové komunikace a hlášení.
d) Komunikační matice s klíčovými osobami pro jednotlivé služby.
e) Eskalační postupy pro krizové situace.
f) Postupy pro spuštění a ukončení chodu systému, pro restart nebo obnovení chodu systému po selhání a pro ošetření chybových stavů nebo mimořádných jevů.
g) Způsob a perioda testování jednotlivých plánu kontinuity činností a plánů obnovy.
h) Postupy pro realizaci opatření vydaných Úřadem.

1.14. Politika fyzické bezpečnosti
a) Stanovení fyzických bezpečnostních perimetrů.
b) Pravidla a postupy pro ochranu 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.

1.15. Politika bezpečnosti komunikační sítě
   a) Pravidla a postupy pro zajištění segmentace sítě a oddělení jednotlivých prostředí
   b) Pravidla, práva a oprávnění pro jednotlivá 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 dodavateli nebo jinými osobami.
   f) Pravidla a postupy pro vzdálenou správu technických aktiv, a to včetně vzdálené správy technických aktiv dodavatelem nebo jinými osobami.

1.16. Politika pro zaznamenávání událostí
   a) Pravidla a postupy pro určování technických aktiv, u kterých je zaznamenávání bezpečnostních a relevantních provozních událostí prováděno, a určení osoby odpovědné za aktuálnost těchto technických aktiv.
   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 jednotného času technických aktiv.
   g) Pravidla pro retenci zaznamenaných událostí.
   h) Opatření pro ochranu přístupu k pořizovaným záznamům.

1.17. Politika nasazení, používání a údržby nástrojů pro detekci 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.

1.18. Politika aplikační bezpečnosti, 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 Pravidla a postupy testování aktualizací, záplat a nových verzí programových prostředků a vybavení včetně postupů a procesů pro případné nespěšné nasazení a obnovení původního stavu (rollback).
   e) Pravidla a postupy pro skenování zranitelností a práci s nálezy.
   f) Pravidla a postupy pro penetrační testování a práci s jeho nálezy.

1.19. 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).

1.20. 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. Zpráva o přezkoumání zajišťování minimální úrovně kybernetické bezpečnosti
a) Vyhodnocení bezpečnostních opatření z předchozího přezkoumání zajišťování minimální úrovně kybernetické bezpečnosti.
b) Identifikace změn a okolností, které mohou mít vliv na zajišťování minimální úrovně kybernetické bezpečnosti.
c) Zpětná vazba o účinnosti řízení bezpečnosti informací
1) neshody a nápravná opatření,
2) výsledky monitorování a měření,
3) výsledky provedených inspekcí v oblasti kybernetické bezpečnosti,
4) naplnění strategických cílů zajišťování minimální úrovně kybernetické bezpečnosti.
d) Posouzení stavu plánu zavádění bezpečnostních opatřeních.
e) Posouzení dopadů kybernetických bezpečnostních incidentů na poskytované služby a kybernetickou bezpečnost.
f) Posouzení změn, které mohou mít negativní dopad na zajišťování minimální úrovně kybernetické bezpečnosti.
g) Identifikace možností pro neustálé zlepšování.
h) Doporučení potřebných rozhodnutí, stanovení bezpečnostních opatření a osob zajišťujících výkon jednotlivých činností.

2.2. 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.

2.3. Přehled bezpečnostních opatření
a) Přehled bezpečnostních opatření požadovaných touto vyhláškou, která nebyla aplikována včetně odůvodnění, proč nebyla aplikována.
b) Přehled aplikovaných bezpečnostních opatření, včetně způsobu jejich realizace.

2.4. Plán zavádění bezpečnostních opatření
   a) Cíle a přínosy vybraných bezpečnostních opatření.
   b) Potřebné zdroje pro jednotlivá bezpečnostní opatření.
   c) Osoby zajišťující prosazování jednotlivých bezpečnostních opatření.
   d) Termíny zavedení jednotlivých bezpečnostních opatření.
   e) Způsob realizace bezpečnostních opatření.

2.5. 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.

2.6. 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.

2.7. Metodika pro provedení analýzy dopadů
   a) Způsoby hodnocení dopadů kybernetických bezpečnostních incidentů na kontinuitu.

2.8. 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.

2.9. Plány obnovy
   a) Umístění a popis záloh.
   b) Detailní postupy pro obnovení dat včetně pořadí činností, odpovědných osob, potřebného času a zdrojů.
   c) Způsob ověření úspěšného obnovení dat ze zálohy.

2.10. 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.

2.11. Další doporučená dokumentace
   a) Topologie infrastruktury.
   b) Segmentace infrastruktury.
   c) Stanovení fyzického bezpečnostního perimetru.
   d) Přehled technických aktiv zejména síťových zařízení, aktivních prvků, koncových zařízení a serverů.
   e) Spojení na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory.

**Příloha č. 4 k vyhlášce č. XX/XXXX Sb.**

**Požadavky na smluvní ujednání s dodavateli**

Obsah smlouvy uzavírané s dodavateli stanoví způsoby realizace bezpečnostních opatření a určuje obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření.

Doporučená bezpečnostní opatření pro smluvní vztahy s dodavateli informačních a operačních technologií:

a) ustanovení zajišťující bezpečnosti informací (požadavek na zajištění důvěrnosti, dostupnosti a integrity),
b) ustanovení o kontrole a auditu dodavatele,
c) ustanovení o řetězení dodavatelů,
d) ustanovení upravující tzv. exit strategii, podmínky ukončení smluvního vztahu z pohledu bezpečnosti,
e) ustanovení o sankcích za porušení smluvních povinností,
f) ustanovení o oprávnění užívat data,
g) ustanovení o autorství programového kódu, případně o programových licencích,
h) ustanovení o důvěrnosti smluvního vztahu,
i) ustanovení upravující povinnost dodržovat pravidla pro dodavatele, se kterými byli relevantní pracovníci dodavatele prokazatelně seznámeni,
j) ustanovení o řízení změn,
k) ustanovení o kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy,
l) ustanovení upravující zajištění řízení kontinuity činností.

Povinné osobě je doporučeno požadovat při uzavírání smluv s dodavateli i další ujednání zohledňující specifické požadavky plynoucí ze zajištění provozních a bezpečnostních potřeb souvisejících s regulovanou službou neuvedené v této příloze.

**Příloha č. 5 k vyhlášce č. XX/XXXX Sb.**

**VZOR: Plán kontinuity činností**

| **PLÁN KONTINUITY ČINNOSTÍ (BCP)** | |
|---|---|
| **Krizový scénář** | Přívalová povodeň |
| **Nebezpečí** | Zničení serverovny, ztráta dat. |
| **Platné pro** | *výpis relevantních odpovědných osob (např. ředitel odboru informačních a komunikačních technologií, manažer kybernetické bezpečnosti, garanti příslušných aktiv atd.)* |
| **OPATŘENÍ** | |
| **Prevence a bezpečnostní opatření pro snížení dopadu v případě aktivace hrozby** | |
| 1. Umístění serverovny do vyšších pater budovy.<br>2. Vytvoření záloh, ze kterých by bylo možné obnovit provoz v jiné lokalitě.<br>3. Nasmlouvání záložní lokality. V případě vzniku mimořádné události přesun do alternativní (záložní) lokality. | |
| **Činnosti v případě aktivace zdroje hrozby**<br>Scénář pokrývá nejhorší variantu, kdy bude nutné opustit budovu společnosti, ve které je uložena serverovna. V rámci testování i v průběhu ostrého nasazení plánu kontinuity činností musí být veškeré činnosti obnovy dokumentovány, aby mohly být zde uvedené postupy obnovy případně aktualizovány nebo upřesněny – provádí určený člen týmu. | **Doba trvání** |
| 1. Svolání krizového týmu společnosti<br>– Svolání krizového týmu.Postup dle povodňového plánu společnosti.<br>– Rozhodnutí o aktivaci záložní lokality, utlumení činnosti organizace a evakuaci osob. | 1 hod. |
| 2. Zahájení přípravy spuštění záložní lokality<br>– Aplikace opatření pro minimalizaci škod v hlavní lokalitě.<br>– Sbalení vytvořených záloh na základě plánu obnovy.<br>– Přesun odpovědných osob do záložní lokality – pracovníci odboru informačních a komunikačních technologií, a další členové týmu potřební pro zachování chodu nezbytných činností společnosti.<br>– Instalace a konfigurace serverů, aplikací, síťových prvků na základě plánu obnovy.<br>– Spuštění provozu v záložní lokalitě (případně v omezeném režimu). | 5 hod. |
| 3. Zahájení ostrého provozu v záložní lokalitě<br>– Informování vedení společnosti o obnovení provozu v záložní lokalitě, případně o omezení provozních kapacit nebo jiných omezeních | 1 hod. |

| | |
|---|---|
| **Konec (Celková doba trvání)** | **7 hod.** |
| **Doporučení pro méně závažný vývoj situace** | |
| V případě, že se krizový štáb rozhodne neaktivovat záložní lokalitu, bude utlumena činnost organizace, budou podniknuta opatření pro minimalizaci škod (protipovodňová opatření), všechny osoby budou evakuovány. | |
| **Další postup** | |
| Mimořádná událost bude nadále monitorována. Po opadnutí povodně začnou likvidační práce a obnovení činností organizace v plném rozsahu. | |

**Příloha č. 6 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