Návrh

VYHLÁŠKA

ze dne ………. 2025

o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností

Národní úřad pro kybernetickou a informační bezpečnost stanoví podle § 13 odst. 3 a § 15 odst. 3 zákona č. [*bude doplněno*] Sb., o kybernetické bezpečnosti (dále jen „zákon“):

## ČÁST PRVNÍ **ÚVODNÍ USTANOVENÍ**

#### § 1 Předmět úpravy

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

1. obsah a rozsah bezpečnostních opatření a
2. stanovení významnosti dopadu kybernetického bezpečnostního incidentu.

*CELEX 32022L2555*

§ 2  
Vymezení pojmů

Pro účely této vyhlášky se rozumí

1. uživatelem fyzická nebo právnická osoba nebo orgán veřejné moci, který využívá aktiva,
2. administrátorem privilegovaný uživatel nebo osoba zajišťující správu, provoz, použití, údržbu a bezpečnost technického aktiva,
3. privilegovaným uživatelem orgán nebo osoba, jejichž činnost na technickém aktivu může mít významný dopad na bezpečnost regulované služby,
4. bezpečnostní politikou soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv

*CELEX 32022L2555*

## ČÁST DRUHÁ **BEZPEČNOSTNÍ OPATŘENÍ**

§ 3

Povinná osoba zavede a provádí bezpečnostní opatření podle této vyhlášky v rozsahu řízení kybernetické bezpečnosti stanoveném podle § 12 zákona v míře nezbytné pro zajištění kybernetické bezpečnosti regulované služby.

*CELEX 32022L2555*

§ 4  
Systém zajišťování minimální kybernetické bezpečnosti

1. Povinná osoba při zajišťování kybernetické bezpečnosti
2. zavede a provádí bezpečnostní opatření v souladu s § 3, která jsou přiměřená bezpečnostním potřebám a
3. vždy zavede a provádí alespoň bezpečnostní opatření podle § 4 odst. 2 až 6, § 5 až 7 a 11.
4. Povinná osoba
5. zpracuje přehled bezpečnostních opatření podle přílohy č. 1 k této vyhlášce, který obsahuje
6. přehled všech bezpečnostních opatření, která byla povinnou osobou zavedena, včetně popisu jejich zavedení,
7. přehled všech bezpečnostních opatření, která budou povinnou osobou zavedena, včetně termínů pro jejich zavedení, priority jejich zavedení a určení osoby odpovědné za jejich zavedení, a
8. přehled všech bezpečnostních opatření, která nebyla zavedena, včetně odůvodnění jejich nezavedení,
9. provede a dokumentuje alespoň jednou ročně vyhodnocení účinnosti zavedených bezpečnostních opatření, včetně aktualizace přehledu bezpečnostních opatření,
10. uchovává jednotlivé přehledy bezpečnostních opatření, alespoň po dobu 4 let.
11. Povinná osoba v rámci řízení bezpečnostní politiky a bezpečnostní dokumentace
12. stanoví bezpečnostní politiku a bezpečnostní dokumentaci k bezpečnostním opatřením požadovaným touto vyhláškou,
13. pravidelně přezkoumává a aktualizuje pravidla a postupy stanovené v bezpečnostní politice a bezpečnostní dokumentaci a
14. vynucuje dodržování pravidel a postupů stanovených v bezpečnostní politice a bezpečnostní dokumentaci.
15. Povinná osoba v rámci řízení aktiv stanoví pravidla pro používání a manipulaci technických aktiv.
16. Povinná osoba při uzavírání smlouvy s dodavateli zajistí, aby smlouvy s těmito dodavateli obsahovaly relevantní požadavky na smluvní ujednaní uvedené v příloze č. 2 k této vyhlášce.
17. Povinná osoba v souvislosti s plánovanou akvizicí, vývojem a údržbou technických aktiv stanoví bezpečnostní požadavky v oblasti kybernetické bezpečnosti a vymáhá jejich dodržování, přičemž vychází z požadavků na bezpečnostní opatření podle této vyhlášky.

*CELEX 32022L2555*

§ 5  
Požadavky na vrcholné vedení

Statutární orgán nebo jiná osoba nebo skupina osob v obdobném postavení (dále jen „vrcholné vedení“) s ohledem na zajišťování kybernetické bezpečnosti

1. určí osobu pověřenou kybernetickou bezpečností, která je pověřená řízením a rozvojem kybernetické bezpečnosti, dohledem nad stavem kybernetické bezpečnosti a komunikací s vrcholným vedením, přičemž pověřena může být osoba, která pro tuto činnost
2. bez zbytečného odkladu absolvuje odborné školení podle § 6 odst. 2 písm. d), nebo
3. prokáže odbornou znalost v kybernetické bezpečnosti,
4. absolvuje prokazatelně školení podle § 6 odst. 2 písm. a),
5. zajistí dostupnost zdrojů potřebných pro zajišťování kybernetické bezpečnosti v souladu s přehledem bezpečnostních opatření,
6. se seznamuje prokazatelně se stavem plnění bezpečnostních opatření uvedeným v přehledu bezpečnostních opatření podle § 4 odst. 2 písm. a),
7. prosazuje neustálé zlepšování zajišťování kybernetické bezpečnosti a za tímto účelem podporuje osobu pověřenou kybernetickou bezpečností a jiné relevantní osoby a
8. stanoví prioritu obnovy primárních aktiv.

*CELEX 32022L2555*

§ 6  
Bezpečnost lidských zdrojů

1. Povinná osoba v rámci bezpečnosti lidských zdrojů
   1. stanoví politiku bezpečného chování uživatelů, v rámci které zohledňuje relevantní témata uvedená v příloze č. 3 k této vyhlášce,
   2. stanoví pravidla rozvoje bezpečnostního povědomí vrcholného vedení, uživatelů, administrátorů a osoby pověřené kybernetickou bezpečností, včetně pravidel pro tvorbu hesel,
   3. zajistí kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osoby pověřené kybernetickou bezpečností a
   4. stanoví pravidla a postupy pro řešení případů porušení bezpečnostní politiky.
2. Povinná osoba v souladu s pravidly rozvoje bezpečnostního povědomí zajistí
   1. poučení vrcholného vedení o jeho povinnostech a o bezpečnostní politice, zejména v oblasti zajišťování kybernetické bezpečnosti formou vstupních a pravidelných školení,
   2. vstupní školení v oblasti kybernetické bezpečnosti,
   3. pravidelná školení v oblasti kybernetické bezpečnosti a
   4. potřebná odborná teoretická i praktická školení administrátorů a osoby pověřené kybernetickou bezpečností v souladu s jejich pracovní náplní.
3. Povinná osoba vede přehledy o provedených školeních a seznamy školených osob podle odstavce 2.

*CELEX 32022L2555*

§ 7  
Řízení kontinuity činností

Povinná osoba v rámci řízení kontinuity činností

1. stanoví prioritu technických aktiv, pořadí a postupy jejich obnovy a zohlední přitom stanovenou prioritu relevantního primárního aktiva podle § 5 písm. f),
2. stanoví dílčí odpovědnosti a povinnosti pro zajištění kontinuity činností a k obnově podle písmene a), a
3. vytváří pravidelné zálohy informací, dat, konfigurací a nastavení technických aktiv nezbytných zejména pro účely obnovy regulované služby pro případ kybernetického bezpečnostního incidentu.

*CELEX 32022L2555*

§ 8  
Řízení přístupu

1. Povinná osoba řídí přístup k aktivům a v rámci něj
2. přidělí každému uživateli a administrátorovi přistupujícímu k aktivům přístupová práva a oprávnění na úroveň nezbytně nutnou k výkonu práce a jedinečný identifikátor daného typu účtu, přičemž odděluje uživatelské a administrátorské účty jedné osoby,
3. řídí identifikátory, přístupová práva a oprávnění účtů technických aktiv,
4. 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,
5. provádí pravidelné přezkoumání nastavení veškerých přístupových práv a oprávnění,
6. zajistí bezodkladné odebrání nebo změnu přístupových práv a oprávnění při změně pozice nebo zařazení uživatelů nebo administrátorů a
7. zajistí deaktivaci účtu a bezodkladné odebrání nebo změnu přístupových práv a oprávnění při ukončení nebo změně smluvního vztahu, na základě kterého došlo ke zřízení přístupu k aktivům.
8. Povinná osoba v rámci zajištění fyzické bezpečnosti zamezí neoprávněnému přístupu ke svým aktivům a předchází poškození, odcizení, zneužití aktiv, neoprávněným zásahům do nich a narušení bezpečnosti poskytování regulované služby.

*CELEX 32022L2555*

§ 9  
Řízení identit a jejich oprávnění

1. Povinná osoba pro řízení identit, přístupových práv a oprávnění používá nástroj, který zajišťuje
2. řízení počtu možných neúspěšných pokusů o přihlášení,
3. opětovné ověření identity po stanovené době nečinnosti,
4. odolnost uložených a přenášených autentizačních údajů a
5. řízení přístupových práv, oprávnění pro čtení a zápis informací a dat a změnu oprávnění.
6. Povinná osoba pro ověření identity administrátorů a uživatelů využívá autentizační mechanismus, který je založený na vícefaktorové autentizaci s alespoň dvěma různými typy faktorů, nebo využívá autentizační mechanismus, který je založený na aktuálně odolné kontinuální autentizaci založené na modelu nulové důvěry.
7. Povinná osoba do doby využívání autentizačního mechanismu podle odstavce 2, využívá autentizaci pomocí kryptografických klíčů nebo certifikátů.
8. Povinná osoba do doby využívání autentizačního mechanismu podle odstavce 3, využívá nástroj založený na autentizaci pomocí identifikátoru účtu a hesla, kdy tento nástroj musí vynucovat pravidla
9. délky hesla alespoň
10. 12 znaků pro účty uživatelů,
11. 17 znaků pro účty administrátorů,
12. 22 znaků pro účty technických aktiv,
13. bezodkladné změny výchozího hesla pro ověření identity technických aktiv, přičemž nové heslo musí být vytvořeno náhodným řetězcem složeným z malých a velkých písmen, číslic a speciálních znaků,
14. neomezující použití malých a velkých písmen, číslic a speciálních znaků,
15. povinné změny hesla v intervalu alespoň jednou za 18 měsíců a
16. neumožňující uživatelům a administrátorům
17. zvolit si jednoduchá a často používaná hesla,
18. tvořit hesla na základě mnohonásobně opakujících se znaků, přihlašovacích jmen, adres elektronické pošty, názvů systémů nebo obdobným způsobem a
19. opětovného použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel.
20. Povinná osoba při řízení identit dále zajistí
21. důvěrnost při vytváření výchozích autentizačních údajů a při obnově přístupu,
22. změnu výchozího hesla nebo hesla sloužícího k obnově přístupu po jeho prvním použití,
23. zneplatnění hesla nebo identifikátoru sloužícího k obnově přístupu nejpozději do 24 hodin od jeho vytvoření,
24. bezodkladnou změnu přístupového hesla v případě důvodného podezření na jeho kompromitaci a
25. zabezpečení administrátorských účtů technických aktiv zejména určených pro případ obnovy po kybernetickém bezpečnostním incidentu a využívá tyto účty pouze nezbytně nutných případech.

*CELEX 32022L2555*

§ 10  
Detekce a zaznamenávání kybernetických bezpečnostních událostí

1. Povinná osoba při detekci kybernetických bezpečnostních událostí zajistí
2. ověření a kontrolu přenášených dat na perimetru komunikační sítě, včetně blokování nežádoucí komunikace,
3. použití nástroje pro nepřetržitou a automatickou ochranu před škodlivým kódem na technických aktivech, zejména na
4. serverech a
5. koncových stanicích,
6. řízení automatického spouštění obsahu, zejména u vyměnitelných zařízení a datových nosičů,
7. nepřetržité poskytování informací o relevantních detekovaných kybernetických bezpečnostních událostech a včasné varování relevantních osob a
8. pravidelnou a bezodkladnou aktualizaci nástrojů pro nepřetržitou a automatickou ochranu před škodlivým kódem a dalších detekčních nástrojů a jejich pravidel.
9. Povinná osoba za účelem detekce kybernetických bezpečnostních událostí zaznamenává
10. bezpečnostní a relevantní provozní události detekované podle odstavce 1 a bezpečnostní a relevantní provozní události technických aktiv na základě svých bezpečnostních potřeb a
11. u událostí podle odstavce 2 písm. a) následující informace o události
12. datum a čas včetně specifikace časového pásma,
13. typ činnosti,
14. jednoznačnou identifikaci technického aktiva a identifikaci účtu původce a
15. úspěšnost nebo neúspěšnost činnosti.
16. Povinná osoba uchovává záznamy bezpečnostních a relevantních provozních událostí po dobu, kterou si stanoví na základě svých bezpečnostních potřeb.

*CELEX 32022L2555*

§ 11  
Řešení kybernetických bezpečnostních incidentů

Povinná osoba při řešení kybernetických bezpečnostních událostí a incidentů

1. zajistí, že uživatelé, administrátoři, osoba pověřená kybernetickou bezpečností a další zaměstnanci budou oznamovat neobvyklé chování technických aktiv a podezření na jakékoliv zranitelnosti,
2. vytvoří metodiku pro posuzování kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů, včetně posuzování významnosti dopadu kybernetického bezpečnostního incidentu v souladu s § 15,
3. zajistí detekci kybernetických bezpečnostních událostí,
4. zajistí posuzování kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů v souladu s metodikou podle písmene b),
5. zajistí hlášení kybernetického bezpečnostního incidentu s významným dopadem podle § 15 zákona,
6. zajistí vytvoření závěrečné zprávy o vyřešení kybernetického bezpečnostního incidentu s významným dopadem podle § 16 zákona.

*CELEX 32022L2555*

§ 12  
Bezpečnost komunikačních sítí

Povinná osoba pro ochranu bezpečnosti komunikační sítě, a to zejména jejího síťového perimetru,

1. zajistí segmentaci komunikační sítě, včetně oddělení provozního a zálohovacího prostředí,
2. omezí odchozí a příchozí komunikaci na perimetru komunikační sítě na nezbytně nutnou pro řádné zajištění poskytování regulované služby,
3. užívá aktuálně odolné a bezpečné komunikační protokoly,
4. v případě užití vzdáleného připojení do interní komunikační sítě nebo vzdálené správy technických aktiv regulované služby
5. omezí tato připojení na nezbytně nutná,
6. zavede bezpečnostní opatření, která zajistí důvěrnost a integritu těchto vzdálených připojení a vzdálené správy a
7. má přehled o uživatelích a administrátorech, kteří tato vzdálená připojení nebo vzdálenou správu užívají.

*CELEX 32022L2555*

§ 13  
Aplikační bezpečnost

Povinná osoba při zajišťování aplikační bezpečnosti regulované služby

1. zajistí bezodkladné aplikování schválených bezpečnostních aktualizací vydaných pro technická aktiva,
2. u technických aktiv, která již nejsou výrobcem, dodavatelem nebo jinou osobou podporována
3. vede jejich evidenci,
4. zavede bezpečnostní opatření, která zaručí obdobnou nebo vyšší úroveň bezpečnosti a
5. omezí jejich komunikaci v komunikační síti na nezbytně nutnou,
6. provádí pravidelné skenování zranitelností relevantních technických aktiv a aplikuje přiměřená bezpečnostní opatření na základě zjištěných výsledků.

*CELEX 32022L2555*

§ 14  
Kryptografické algoritmy

1. Povinná osoba při zajištění bezpečnosti technických aktiv a jejich komunikace
2. používá aktuálně odolné kryptografické algoritmy,
3. prosazuje bezpečné nakládání s kryptografickými algoritmy a
4. zohledňuje doporučení a metodiky v oblasti kryptografických algoritmů vydané Národním úřadem pro kybernetickou a informační bezpečnost.
5. Povinná osoba zajišťuje bezpečnou
6. hlasovou, audiovizuální a textovou komunikaci, a to včetně e-mailové komunikace a
7. nouzové komunikace v rámci organizace.

*CELEX 32022L2555*

ČÁST TŘETÍ  
STANOVENÍ VÝZNAMNOSTI DOPADU KYBERNETICKÉHO BEZPEČNOSTNÍHO INCIDENTU

§ 15

1. Povinná osoba pro potřeby vyhodnocení významnosti dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby stanoví
2. únosnou míru újmy způsobené kybernetickým bezpečnostním incidentem, v jehož důsledku ještě není ohrožen život nebo zdraví osob nebo schopnost povinné osoby dostát svým závazkům,
3. oblasti pro posouzení významnosti dopadu kybernetických bezpečnostních incidentů zohledňující zejména
4. provozní dopad kybernetického bezpečnostního incidentu na povinnou osobu a její schopnost poskytovat regulovanou službu,
5. množství uživatelů regulované služby a jiných orgánů a osob zasažených kybernetickým bezpečnostním incidentem,
6. časové, lidské a technické zdroje, které jsou potřebné k obnově poskytování zasažené regulované služby,
7. typ a umístění aktiv dotčených kybernetickým bezpečnostním incidentem,
8. citlivost informací a dat zasažených kybernetickým bezpečnostním incidentem a újmu, jakou může narušení bezpečnosti těchto informací a dat způsobit povinné osobě nebo jinému orgánu nebo osobě a
9. přímou příčinu kybernetického bezpečnostního incidentu, je-li povinné osobě známa, zda se jedná o lidskou chybu, technickou závadu nebo úmyslné jednání.
10. Dopad kybernetického bezpečnostního incidentu na poskytování regulované služby je považován za významný, pokud
11. přesáhne povinnou osobou stanovenou únosnou míru újmy způsobenou kybernetickým bezpečnostním incidentem podle odstavce 1 písm. a) a zároveň
12. je oblast pro posouzení významnosti dopadu podle odstavce 1 písm. b) posouzena jako významná.

ČÁST ČTVRTÁ  
ÚČINNOST

§ 16  
Účinnost

Tato vyhláška nabývá účinnosti dnem [*bude doplněno ve spolupráci se Sbírkou a v návaznosti na účinnost zákona, k jehož provedení se vyhláška vydává*].

Ředitel:

Ing. Lukáš Kintr

Příloha č. 1 k vyhlášce č. …/2025 Sb.

**Přehled bezpečnostních opatření**

Tato příloha představuje přehled bezpečnostních opatření ve formě tabulky (Tab. č. 1), která má povinné osobě sloužit jako nástroj k vyhodnocení účinnosti zavedených bezpečnostních opatření za stanovené období.

**Tab. č. 1: Přehled bezpečnostních opatření**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Vyhodnocení účinnosti zajišťování kybernetické bezpečnosti** | | | | |  |
| **Bezpečnostní opatření podle vyhlášky** | **Stav bezpečnostního opatření** | **Popis bezpečnostního opatření** | **Termín zavedení bezpečnostního opatření** | **Priorita zavedení bezpečnostního opatření** | **Odpovědnost za bezpečnostní opatření** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Přehled bezpečnostních opatření je složen ze šesti sloupců, kdy specifika jednotlivých sloupců a příklady jejich vyplnění jsou uvedeny v tabulkách níže (Tab.č. 2 až 7). V Tabulce č. 3 „Stav bezpečnostního opatření“ jsou místo příkladů uvedeny „Přípustné hodnoty“.

**Tab. č. 2: Bezpečnostní opatření podle vyhlášky**

|  |  |
| --- | --- |
| **Název sloupce v Tab. č. 1** | Bezpečnostní opatření podle vyhlášky. |
| **Popis sloupce** | Příslušné bezpečnostní opatření požadované vyhláškou uvedené například formou odkazu na dotčené ustanovení vyhlášky. |
| **Popis hodnot** | Uvedené hodnoty musí splňovat základní strukturu uváděnou v právních předpisech, přičemž je doporučeno, aby byly jednotlivé části uvedeny v logické návaznosti. |
| **Příklad** | § 6 písm. a) |
| § 9 odst. 4 písm. a) bod 2 |
| § 9 odst. 4 písm. a) až e) |

**Tab. č. 3: Stav bezpečnostních opatření**

|  |  |
| --- | --- |
| **Název sloupce v Tab. č. 1** | Stav bezpečnostního opatření. |
| **Popis sloupce** | Popis stavu bezpečnostního opatření ve chvíli, kdy je provedeno vyhodnocení účinnosti zajišťování kybernetické bezpečnosti. |
| **Popis hodnot** | Hodnotu „zavedeno“ lze zapsat v případě, kdy bylo bezpečnostní opatření v hodnoceném období zavedeno v požadovaném rozsahu. |
| Hodnotu „v procesu“ lze zapsat v případě, kdy je bezpečnostní opatření (nebo jeho část) v hodnoceném období zaváděno, popřípadě jsou činěny doložitelné kroky k jeho zavedení (například výběrové řízení, smlouva, testovací provoz atd.) |
| Hodnotu „nezavedeno“ lze zapsat pouze v případě, kdy opatření zavedeno nebylo. |
| **Přípustné hodnoty** | Zavedeno |
| V procesu |
| Nezavedeno |

**Tab. č. 4: Popis bezpečnostního opatření**

|  |  |
| --- | --- |
| **Název sloupce v Tab. č. 1** | Popis bezpečnostního opatření. |
| **Popis sloupce** | Stručný popis zavedení bezpečnostního opatření v návaznosti na stav, v jakém se aktuálně nachází, a s přihlédnutím k prostředí povinné osoby. |
| **Popis hodnot** | Popis jednotlivých bezpečnostních opatření by měl stručně reflektovat situaci u povinné osoby (například podle názvů příslušných částí bezpečnostní dokumentace) a stav bezpečnostního opatření podle Tab. č. 2. |
| V případě bezpečnostních opatření, která jsou označena jako „v procesu“ je nutné popsat prozatímní stav, případně uvést odkaz na dokumentaci, která proces zavádění dokládá. |
| Pokud je bezpečnostní opatření označeno jako „nezavedeno“, je nutné odůvodnit, proč zavedeno nebylo. |
| **Příklad** | Politika bezpečného chování uživatelů je v dokumentu BP04\_Bezp\_lidskych\_zdroju v kapitole „1 - Politika bezpečného chování uživatelů“ a jsou v ní zohledněna relevantní témata z přílohy č. 3 k této vyhlášce. |
| Dvoufaktorové ověření, založeno na OTP a PIN, je zavedeno v systému ZY v testovacím provozu u zaměstnanců disponujících služebním mobilním telefonem, na kterém je nainstalována aplikace s OTP. |
| Bude zavedeno až po kompletní výměně koncových stanic – na aktuální hardware aplikace XZ nasadit nelze. |
| Není relevantní pro danou službu. |
| Nelze zavést na technickém aktivu XY z důvodu, že toto aktivum tuto funkcionalitu nepodporuje. |

**Tab. č. 5: Termín zavedení bezpečnostního opatření**

|  |  |
| --- | --- |
| **Název sloupce v Tab. č. 1** | Termín zavedení bezpečnostního opatření. |
| **Popis sloupce** | Plánovaný termín zavedení bezpečnostního opatření v plném rozsahu. |
| **Popis hodnot** | Tato hodnota bude vyplněna pouze v případě, je-li stav bezpečnostního opatření označen jako „v procesu“ nebo „nezavedeno“, ale jeho zavedení je v budoucnu plánováno nebo závisí na dalších okolnostech. |
| **Příklad** | leden 2025 |
| 15. ledna 2025 |
| Q1 2025 |
| Q1/Q2 2025 |

**Tab. č. 6: Priorita zavedení bezpečnostního opatření**

|  |  |
| --- | --- |
| **Název sloupce v Tab. č. 1** | Priorita zavedení bezpečnostního opatření. |
| **Popis sloupce** | Prioritizace zavádění bezpečnostních opatření s ohledem na dopad na poskytování regulované služby. |
| **Popis hodnot** | Hodnotu „nízká“ nebo „1“ je možné zapsat v případě, kdy by absence zavedení bezpečnostního opatření neměla dopad na poskytování regulované služby nebo dané bezpečnostní opatření není pro poskytování regulované služby relevantní. |
| Hodnotu „střední“ nebo „2“ je možné zapsat v případě, kdy by absence zavedení bezpečnostního opatření měla minimální a krátkodobý dopad na poskytování regulované služby. |
| Hodnotu „vysoká“ nebo „3“ je možné zapsat v případě, kdy by absence zavedení bezpečnostního opatření měla za následek vážný a dlouhodobý dopad na poskytování regulované služby. |
| Hodnotu „kritická“ nebo „4“ je možné zapsat v případě, kdy by absence zavedení bezpečnostního opatření měla okamžité a nevratné důsledky pro poskytování regulované služby nebo jsou známy úspěšné pokusy o překonání bezpečnostních opatření. |
| **Příklad** | Nízká (obdobně lze vyjádřit číselnou hodnotou, například „1“). |
| Střední (obdobně lze vyjádřit číselnou hodnotou, například „2“). |
| Vysoká (obdobně lze vyjádřit číselnou hodnotou, například „3“). |
| Kritická (obdobně lze vyjádřit číselnou hodnotou, například „4“). |

**Tab. č. 7: Odpovědnost za bezpečnostní opatření**

|  |  |
| --- | --- |
| **Název sloupce v Tab. č. 1** | Odpovědnost za bezpečnostní opatření. |
| **Popis sloupce** | Osoba pověřená za zavedení daného bezpečnostního opatření. |
| **Popis hodnot** | Je nutné zaznamenat údaje tak, aby bylo možné jednoznačně určit osobu pověřenou za zavedení bezpečnostního opatření. V případě potřeby je možné uvést také konkrétní organizační složku do níž daná osoba spadá. |
| **Příklad** | Titul, jméno, příjmení, organizační složka. |

Příloha č. 2 k vyhlášce č. …/2025 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.

Obsah smlouvy s dodavateli musí obsahovat relevantní ustanovení z níže uvedených:

1. ustanovení o bezpečnosti informací z pohledu důvěrnosti (včetně ustanovení o mlčenlivosti), integrity a dostupnosti,
2. ustanovení o auditu dodavatele,
3. ustanovení o řetězení dodavatelů,
4. ustanovení upravující tzv. exit strategii, podmínky ukončení smluvního vztahu z pohledu bezpečnosti informací,
5. ustanovení o sankcích za porušení smluvních povinností,
6. ustanovení o oprávnění užívat data,
7. ustanovení o autorství programového kódu, případně o programových licencích,
8. ustanovení o důvěrnosti smluvního vztahu,
9. ustanovení upravující povinnost dodržovat pravidla pro dodavatele, se kterými byli relevantní pracovníci dodavatele prokazatelně seznámeni,
10. ustanovení o řízení změn,
11. ustanovení o kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy,
12. ustanovení upravující zajištění řízení kontinuity činností,
13. náležitosti smlouvy o úrovni služeb (SLA) a způsobu a úrovni realizace bezpečnostních opatření.

Povinná osoba může požadovat při uzavírání smluv s dodavateli i další ujednání zohledňující specifické požadavky plynoucí ze zajištění provozních a bezpečnostních potřeb souvisejících s regulovanou službou, která nejsou uvedena v této příloze.

Příloha č. 3 k vyhlášce č. …/2025 Sb.

**Doporučená témata pro rozvoj bezpečnostního povědomí**

1. Techniky zabezpečení zařízení.
2. Firewall, antivirový program a jejich omezení.
3. Škodlivé programy a jejich projevy.
4. Rizika stahování programů a aplikací.
5. Aktualizace software.
6. Rizika povolení a zakázání spouštění maker.
7. Rizika spustitelných souborů.
8. Zásady zabezpečení uživatelských účtů.
9. Používání, tvorba a správa hesel.
10. Vícefaktorová autentizace.
11. Techniky sociálního inženýrství.
12. On-line identita, digitální stopa a její minimalizace.
13. Zásady práce v počítačové síti.
14. Používání vzdáleného připojení (VPN).
15. Bezpečná elektronická komunikace.
16. Bezpečnost webových stránek.
17. Zálohování, ukládání a šifrování dat.
18. Bezpečné používání přenosných technických nosičů dat.
19. Využívání služeb cloud computingu.
20. Pravidla a postupy pro oznamování neobvyklého chování technických aktiv a podezření na jakékoliv zranitelnosti.
21. Základní postup při reakci na kybernetickou bezpečnostní událost nebo kybernetický bezpečnostní incident.
22. Zásady bezpečného používání pracovních zařízení pro soukromé účely.
23. Zásady bezpečného používání soukromých zařízení pro pracovní účely (tzv. BYOD).
24. Osobní odpovědnost zaměstnance při dodržování zásad kybernetické bezpečnosti.
25. Aktuální hrozby v kybernetické bezpečnosti.

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). [↑](#footnote-ref-1)