ZÁKONY PRO LIDI

Vyhláška č. 410/2025 Sb.

Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností

https://www.zakonyprolidi.cz/cs/2025-410

Částka	**410/2025**
Platnost od	**14.10.2025**
Účinnost od	**01.11.2025**

Aktuální znění 01.11.2025

410

VYHLÁŠKA

ze dne 26. září 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. 264/2025 Sb., o kybernetické bezpečnosti, (dále jen „zákon“):

ČÁST PRVNÍ

ÚVODNÍ USTANOVENÍ

§ 1

Předmět 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, způsob zavádění a provádění bezpečnostních opatření a

b) stanovení významnosti dopadu kybernetického bezpečnostního incidentu.

§ 2

Vymezení pojmů

Pro účely této vyhlášky se rozumí

a) uživatelem fyzická nebo právnická osoba anebo orgán veřejné moci, který využívá aktiva,

b) privilegovaným uživatelem uživatel nebo jiná osoba, jejíž činnost na technickém aktivu může mít významný dopad na bezpečnost regulované služby,

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

d) bezpečnostní politikou soubor zásad a pravidel, která určují způsob zajištění ochrany aktiv.

ČÁST DRUHÁ

BEZPEČNOSTNÍ OPATŘENÍ

§ 3

Systém zajišťování minimální kybernetické bezpečnosti

(1) Povinná osoba při zajišťování kybernetické bezpečnosti

a) zavede a provádí bezpečnostní opatření, která jsou přiměřená bezpečnostním potřebám, a

b) zavede a provádí alespoň bezpečnostní opatření podle odstavců 2 až 6, § 4 až 6 a § 10.

(2) Povinná osoba

a) stanoví přehled bezpečnostních opatření podle přílohy č. 1 k této vyhlášce, který obsahuje přehled všech

bezpečnostních opatření, která

1. byla povinnou osobou zavedena, včetně popisu jejich zavedení,

2. budou povinnou osobou zavedena, včetně termínů pro jejich zavedení, priority jejich zavedení a určení osoby odpovědné za jejich zavedení, a

3. nebyla zavedena, včetně odůvodnění jejich nezavedení,

b) provede a dokumentuje alespoň jednou ročně aktualizaci přehledu bezpečnostních opatření, včetně vyhodnocení účinnosti zavedených bezpečnostních opatření,

c) uchovává jednotlivé přehledy bezpečnostních opatření a jejich aktualizace alespoň po dobu 4 let.

(3) Povinná osoba v rámci řízení bezpečnostní politiky a bezpečnostní dokumentace

a) stanoví bezpečnostní politiku a bezpečnostní dokumentaci k bezpečnostním opatřením požadovaným touto vyhláškou,

b) pravidelně přezkoumává a aktualizuje pravidla a postupy stanovené v bezpečnostní politice a bezpečnostní dokumentaci a

c) vynucuje dodržování pravidel a postupů stanovených v bezpečnostní politice a bezpečnostní dokumentaci.

(4) Povinná osoba v rámci řízení aktiv stanoví pravidla pro používání a manipulaci technických aktiv.

(5) Povinná osoba při uzavírání smlouvy s dodavatelem do stanoveného rozsahu podle § 12 zákona zohlední hrozby a zranitelnosti spojené s tímto dodavatelem, celkovou kvalitu produktů a postupů v oblasti kybernetické bezpečnosti tohoto dodavatele, včetně postupů bezpečného vývoje a na základě toho zajistí, aby smlouvy s tímto dodavatelem obsahovaly relevantní požadavky na smluvní ujednaní uvedené v příloze č. 2 k této vyhlášce.

(6) 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.

§ 4

Požadavky na vrcholné vedení

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

a) určí osobu pověřenou kybernetickou bezpečností, které svěří pravomoci potřebné k řízení a rozvoji kybernetické bezpečnosti, dohledu nad stavem kybernetické bezpečnosti a komunikaci s vrcholným vedením, přičemž pro výkon této činnosti

1. absolvuje bez zbytečného odkladu odborné školení podle § 5 odst. 2 písm. d), nebo

2. prokáže odbornou znalost v kybernetické bezpečnosti,

b) absolvuje prokazatelně školení podle § 5 odst. 2 písm. a),

c) zajistí dostupnost zdrojů potřebných pro zajišťování kybernetické bezpečnosti v souladu s přehledem bezpečnostních opatření,

d) se prokazatelně seznamuje se stavem plnění bezpečnostních opatření uvedeným v přehledu bezpečnostních opatření podle § 3 odst. 2 písm. a),

e) prosazuje neustálé zlepšování zajišťování kybernetické bezpečnosti a za tímto účelem podporuje osobu pověřenou kybernetickou bezpečností a jiné relevantní osoby a

f) stanoví prioritu obnovy primárních aktiv.

§ 5

Bezpečnost lidských zdrojů

(1) Povinná osoba v rámci bezpečnosti lidských zdrojů

a) stanoví politiku bezpečného chování uživatelů, v jejímž rámci zohledňuje relevantní témata uvedená v příloze č. 3 k této vyhlášce,

b) stanoví pravidla rozvoje bezpečnostního povědomí vrcholného vedení, uživatelů, administrátorů a osoby pověřené kybernetickou bezpečností, včetně pravidel pro tvorbu hesel,

c) zajistí kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osoby pověřené kybernetickou bezpečností a

d) stanoví pravidla a postupy pro řešení případů porušení bezpečnostní politiky.

(2) Povinná osoba v souladu s pravidly rozvoje bezpečnostního povědomí zajistí

a) poučení vrcholného vedení o jeho povinnostech a o bezpečnostní politice, zejména v oblasti zajišťování kybernetické bezpečnosti, formou vstupních a pravidelných školení,

b) vstupní školení v oblasti kybernetické bezpečnosti,

c) pravidelná školení v oblasti kybernetické bezpečnosti a

d) 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.

§ 6

Řízení kontinuity činností

Povinná osoba v rámci řízení kontinuity činností

a) stanoví prioritu technických aktiv, pořadí a postupy jejich obnovy a zohlední přitom stanovenou prioritu relevantního primárního aktiva podle § 4 písm. f),

b) stanoví povinnosti a odpovědnost konkrétních osob za jednotlivé činnosti pro zajištění kontinuity činností a k obnově podle písmene a) a

c) vytváří pravidelné zálohy informací, dat, konfigurací a nastavení technických aktiv nezbytných zejména pro účely obnovy regulované služby pro případ kybernetického bezpečnostního incidentu.

§ 7

Řízení přístupu

(1) Povinná osoba řídí přístup k aktivům a v rámci něj

a) přidělí každému uživateli a administrátorovi přistupujícímu k aktivům přístupová práva a oprávnění na úroveň nezbytně nutnou k výkonu jejich práce a jedinečný identifikátor daného typu účtu, přičemž od sebe odděluje uživatelské a administrátorské účty jedné osoby,

b) řídí identifikátory, přístupová práva a oprávnění účtů technických aktiv,

c) 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,

d) provádí pravidelné přezkoumání nastavení veškerých přístupových práv a oprávnění,

e) zajistí bezodkladné odebrání nebo změnu přístupových práv a oprávnění při změně pozice nebo zařazení uživatelů nebo administrátorů a

f) zajistí deaktivaci účtu a bezodkladné odebrání nebo změnu přístupových práv a oprávnění při ukončení nebo změně smluvního vztahu, na jehož základě došlo ke zřízení přístupu k aktivům.

(2) 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.

§ 8

Řízení identit a jejich oprávnění

(1) Povinná osoba pro řízení identit, přístupových práv a oprávnění používá nástroj, který zajišťuje

a) řízení počtu možných neúspěšných pokusů o přihlášení,

b) opětovné ověření identity po stanovené době nečinnosti,

c) odolnost uložených a přenášených autentizačních údajů a

d) řízení přístupových práv, oprávnění pro čtení a zápis informací a dat a změnu oprávnění.

(2) Povinná osoba pro ověření identity administrátorů, uživatelů a technických aktiv využívá autentizační mechanismus, který je založený na vícefaktorové autentizaci s alespoň dvěma různými typy faktorů, nebo využívá autentizační mechanismus, který je založen na aktuálně odolné kontinuální autentizaci založené na modelu nulové důvěry.

(3) Povinná osoba do doby využívání autentizačního mechanismu podle odstavce 2 využívá autentizaci pomocí kryptografických klíčů nebo certifikátů.

(4) 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

a) délky hesla alespoň

1. 12 znaků pro účty uživatelů,

2. 17 znaků pro účty administrátorů,

3. 22 znaků pro účty technických aktiv,

b) 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,

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

d) povinné změny hesla v intervalu alespoň jednou za 18 měsíců a

e) neumožňující uživatelům a administrátorům

1. zvolit si jednoduchá a často používaná hesla,

2. tvořit hesla na základě mnohonásobně opakujících se znaků, přihlašovacích jmen, adres elektronické pošty, názvů systémů nebo obdobným způsobem a

3. opětovného použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel.

(5) Povinná osoba při řízení identit dále zajistí

a) důvěrnost při vytváření výchozích autentizačních údajů a při obnově přístupu,

b) změnu výchozího hesla nebo hesla sloužícího k obnově přístupu po jeho prvním použití,

c) zneplatnění hesla nebo identifikátoru sloužícího k obnově přístupu nejpozději do 24 hodin od jeho vytvoření,

d) bezodkladnou změnu přístupového hesla v případě důvodného podezření na jeho kompromitaci a

e) zabezpečení administrátorských účtů technických aktiv zejména určených pro případ obnovy po kybernetickém bezpečnostním incidentu a využívá tyto účty pouze v nezbytně nutných případech.

§ 9

Detekce a zaznamenávání kybernetických bezpečnostních událostí

(1) Povinná osoba při detekci kybernetických bezpečnostních událostí zajistí

a) ověření a kontrolu přenášených dat na perimetru komunikační sítě, včetně blokování nežádoucí komunikace,

b) použití nástroje pro nepřetržitou a automatickou ochranu před škodlivým kódem na technických aktivech, zejména na

1. serverech a

2. koncových stanicích,

c) řízení automatického spouštění obsahu, zejména u vyměnitelných zařízení a datových nosičů,

d) nepřetržité poskytování informací o relevantních detekovaných kybernetických bezpečnostních událostech a včasné varování relevantních osob a

e) pravidelnou a bezodkladnou aktualizaci nástrojů pro nepřetržitou a automatickou ochranu před škodlivým kódem a dalších detekčních nástrojů a jejich pravidel.

(2) Povinná osoba za účelem detekce kybernetických bezpečnostních událostí zaznamenává

a) bezpečnostní a relevantní provozní události detekované podle odstavce 1 a bezpečnostní a relevantní provozní události technických aktiv na základě svých bezpečnostních potřeb a

b) u událostí podle písmene a) následující informace o události:

1. datum a čas, včetně specifikace časového pásma,

2. typ činnosti,

3. jednoznačnou identifikaci technického aktiva a identifikaci účtu původce a

4. úspěšnost nebo neúspěšnost činnosti.

(3) Povinná osoba uchovává záznamy bezpečnostních a relevantních provozních událostí po dobu, kterou si stanoví na základě svých bezpečnostních potřeb.

§ 10

Řešení kybernetických bezpečnostních incidentů

Povinná osoba při řešení kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů

a) zajistí, že uživatelé, administrátoři, osoby pověřené kybernetickou bezpečností a další zaměstnanci budou oznamovat neobvyklé chování technických aktiv a podezření na jakékoliv zranitelnosti,

b) vytvoří metodiku pro posuzování kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů, včetně posuzování významnosti dopadu kybernetického bezpečnostního incidentu v souladu s § 14,

c) zajistí detekci kybernetických bezpečnostních událostí,

d) zajistí posuzování kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů v souladu s metodikou podle písmene b),

e) zajistí hlášení kybernetického bezpečnostního incidentu s významným dopadem podle § 15 zákona,

f) zajistí vytvoření závěrečné zprávy o vyřešení kybernetického bezpečnostního incidentu s významným dopadem podle § 16 zákona.

§ 11

Bezpečnost komunikačních sítí

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

a) zajistí segmentaci komunikační sítě, včetně oddělení provozního a zálohovacího prostředí,

b) omezí odchozí a příchozí komunikaci na perimetru komunikační sítě na dobu nezbytně nutnou pro řádné zajištění poskytování regulované služby,

c) užívá aktuálně odolné a bezpečné komunikační protokoly,

d) v případě užití vzdáleného připojení do interní komunikační sítě nebo vzdálené správy technických aktiv regulované služby

1. omezí tato připojení na nezbytně nutná,

2. zavede bezpečnostní opatření, která zajistí důvěrnost a integritu těchto vzdálených připojení a vzdálené správy, a

3. má přehled o uživatelích a administrátorech, kteří tato vzdálená připojení nebo vzdálenou správu užívají.

§ 12

Aplikační bezpečnost

Povinná osoba při zajišťování aplikační bezpečnosti regulované služby

a) zajistí bezodkladné aplikování schválených bezpečnostních aktualizací vydaných pro technická aktiva,

b) u technických aktiv, která již nejsou výrobcem, dodavatelem nebo jinou osobou podporována

1. vede jejich evidenci,

2. zavede bezpečnostní opatření, která zaručí obdobnou nebo vyšší úroveň bezpečnosti, a

3. omezí jejich komunikaci v komunikační síti na nezbytně nutnou,

c) provádí pravidelné skenování zranitelností relevantních technických aktiv a aplikuje přiměřená bezpečnostní opatření na základě zjištěných výsledků.

§ 13

Kryptografické algoritmy

(1) Povinná osoba při zajištění bezpečnosti 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 Národním úřadem pro kybernetickou a informační bezpečnost.

(2) Povinná osoba zajišťuje bezpečnou

a) hlasovou, audiovizuální a textovou komunikaci, a to včetně e-mailové komunikace, a

b) nouzovou komunikaci v rámci organizace.

ČÁST TŘETÍ

STANOVENÍ VÝZNAMNOSTI DOPADU KYBERNETICKÉHO BEZPEČNOSTNÍHO INCIDENTU

§ 14

(1) Povinná osoba pro potřeby vyhodnocení významnosti dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby stanoví

a) únosnou míru újmy způsobené kybernetickým bezpečnostním incidentem, v jehož důsledku ještě není ohrožen život nebo zdraví osob nebo schopnost povinné osoby dostát svým závazkům,

b) oblasti pro posouzení významnosti dopadu kybernetických bezpečnostních incidentů zohledňující zejména

1. provozní dopad kybernetického bezpečnostního incidentu na povinnou osobu a její schopnost poskytovat regulovanou službu,

2. množství uživatelů regulované služby a jiných orgánů a osob zasažených kybernetickým bezpečnostním incidentem,

3. časové, lidské a technické zdroje, které jsou potřebné k obnově poskytování zasažené regulované služby,

4. typ a umístění aktiv dotčených kybernetickým bezpečnostním incidentem,

5. 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

6. přímou příčinu kybernetického bezpečnostního incidentu, je-li povinné osobě známo, zda se jedná o lidskou chybu, technickou závadu nebo úmyslné jednání.

(2) Dopad kybernetického bezpečnostního incidentu na poskytování regulované služby je považován za významný, pokud

a) přesáhne povinnou osobou stanovenou únosnou míru újmy způsobenou kybernetickým bezpečnostním incidentem podle odstavce 1 písm. a) a současně

b) je oblast pro posouzení významnosti dopadu podle odstavce 1 písm. b) posouzena jako významná.

ČÁST ČTVRTÁ

ÚČINNOST

§ 15

Účinnost

Tato vyhláška nabývá účinnosti dnem 1. listopadu 2025.

Ředitel:

Ing. Kintr v. r.

Příloha č. 1

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 odkazovat na konkrétní ustanovení právního předpisu, přičemž je doporučeno, aby byly jednotlivé části uvedeny v logické návaznosti.

Tab. č. 3: Stav bezpečnostního 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	Tento sloupec bude obsahovat právě jednu z přípustných hodnot „Zavedeno“, „V procesu“ nebo „Nezavedeno“.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.

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.

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. Měla by být uvedena buď konkrétním datem nebo kvartálem či měsícem

konkrétního roku.

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.

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.

Příloha č. 2

Požadavky na smluvní ujednání s dodavateli

Povinná osoba uzavírá pouze takové smlouvy, které stanoví způsoby realizace bezpečnostních opatření a určují obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření.

Povinné osoby mohou uzavírat jen takové smlouvy, které budou zohledňovat následující relevantní ustanovení:

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

b) ustanovení o auditu dodavatele související s plněním smlouvy,

c) ustanovení o řetězení dodavatelů,

d) ustanovení upravující tzv. exit strategii, podmínky ukončení smluvního vztahu z pohledu bezpečnosti informací,

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

j) ustanovení o řízení změn,

k) ustanovení o kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy,

l) ustanovení upravující zajištění řízení kontinuity činností,

m) náležitosti smlouvy o úrovni služeb (SLA) a způsobu a úrovni realizace bezpečnostních opatření,

n) ustanovení o dodržování pravidel bezpečného vývoje.

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

Témata pro rozvoj bezpečnostního povědomí

a) Techniky zabezpečení zařízení.

b) Firewall, antivirový program a jejich omezení.

c) Škodlivé programy a jejich projevy.

d) Rizika stahování programů a aplikací.

e) Aktualizace software.

f) Rizika povolení a zakázání spouštění maker.

g) Rizika spustitelných souborů.

h) Zásady zabezpečení uživatelských účtů.

i) Používání, tvorba a správa hesel.

j) Vícefaktorová autentizace.

k) Techniky sociálního inženýrství.

l) On-line identita, digitální stopa a její minimalizace.

m) Zásady práce v počítačové síti.

n) Používání vzdáleného připojení (VPN).

o) Bezpečná elektronická komunikace.

p) Bezpečnost webových stránek.

q) Zálohování, ukládání a šifrování dat.

r) Bezpečné používání přenosných technických nosičů dat.

s) Využívání služeb cloud computingu.

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

u) Základní postup při reakci na kybernetickou bezpečnostní událost nebo kybernetický bezpečnostní incident.

v) Zásady bezpečného používání pracovních zařízení pro soukromé účely.

w) Zásady bezpečného používání soukromých zařízení pro pracovní účely (tzv. BYOD).

x) Osobní odpovědnost zaměstnance při dodržování zásad kybernetické bezpečnosti.

y) Aktuální hrozby v kybernetické bezpečnosti.

Poznámky pod čarou

[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).

Souvislosti

Provádí předpis

264/2025 Sb.	Zákon o kybernetické bezpečnosti (nový)

Je odkazován z

505/2025 Sb.	Vyhláška o některých požadavcích pro zápis do katalogu cloud computingu

Odkazuje na

264/2025 Sb.	Zákon o kybernetické bezpečnosti (nový)

Verze

č.	Znění od - do	Novely	Poznámka
1.	**01.11.2025**		Aktuální znění (exportováno 13.12.2025 13:16)
0.	14.10.2025		Vyhlášené znění