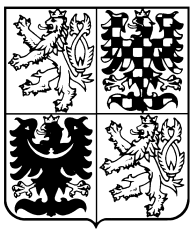


# Sbírka zákonů a mezinárodních smluv

ČESKÁ REPUBLIKA

Zpřístupněna dne 23. června 2025


## Vyhláška č. 202/2025 Sb.

## Vyhláška, kterou se mění vyhláška č. 361/2016 Sb., o zabezpečení jaderného zařízení a jaderného materiálu

# 202

# VYHLÁŠKA

## ze dne 18. června 2025,

## kterou se mění vyhláška č. 361/2016 Sb., o zabezpečení jaderného zařízení a jaderného materiálu

Státní úřad pro jadernou bezpečnost stanoví podle § 236 zákona č. 263/2016 Sb., atomový zákon, ve znění zákona č. 83/2025 Sb., k provedení § 24 odst. 7, § 159 odst. 2, § 159a odst. 5, § 160 odst. 6, § 161 odst. 4 a § 163 odst. 2 písm. a) až c) tohoto zákona:

## Čl. I

Vyhláška č. 361/2016 Sb., o zabezpečení jaderného zařízení a jaderného materiálu, se mění takto:

1. V úvodní větě se za text „§ 159 odst. 2“ vkládá text „ , § 159a odst. 5“ a slova „a b)“ se nahrazují slovy „až c)“.

2. V § 1 se na konci písmene e) slovo „a“ nahrazuje čárkou.

3. V § 1 se na konci písmene f) tečka nahrazuje čárkou a doplňují se písmena g) a h), která znějí:

   „g) rozsah a způsob zajištění, trvalého rozvíjení, udržování a pravidelného hodnocení kultury zabezpečení a

   h) rozsah a způsob zabezpečení počítačového systému nezbytného k řízení jaderné bezpečnosti, evidence jaderných materiálů, fyzické ochrany a zvládání radiační mimořádné události.“.

4. V § 2 písmeno d) zní:

   „d) předmětem ohrožujícím jadernou bezpečnost předmět způsobilý ke zneužití pro účely krádeže, sabotáže nebo jiné neoprávněné činnosti proti jadernému zařízení nebo jadernému materiálu, kterým je zbraň, střelivo, výbušnina, alkoholický nápoj nebo jiná návyková látka, přenosné elektronické zařízení umožňující ovlivnit zpracování informací a zabránit nebo narušit plnění bezpečnostní funkce systému, konstrukce nebo komponenty, nebo jiný předmět, které jsou zahrnuty v projektové základní hrozbě.“.

5. V § 3 se slova „musí být“ nahrazují slovem „je“, za slovo „přílohy“ se vkládá text „č. 1“ a za slovo „příloze“ se vkládá text „č. 1“.

6. V nadpisu § 4 se slovo „Prostory“ nahrazuje slovy „Vymezené prostory“.

7. V § 6 písm. a) bodě 5 se za slovo „vybavena“ vkládá slovo „kamerovým“, slova „průmyslové televize“ se zrušují a slovo „její“ se nahrazuje slovem „jeho“.

8. V § 6 písm. a) bodě 7 se za slovo „a“ vkládá slovo „kamerovým“ a slova „průmyslové televize“ se zrušují.

9. V § 6 písm. b) a c), § 7 odst. 1 písm. b), § 7 odst. 2 a v § 13 odst. 1 se za slovo „narušení,“ vkládá slovo „kamerovým“ a slova „průmyslové televize“ se zrušují.

10. V § 10 odst. 2 se za slovo „do“ vkládá slovo „chráněného,“ a na konci textu odstavce se doplňují slova „a vstup do těchto prostorů je povolen pouze z důvodů vážících se k výkonu zde vykonávaných pracovních činností“.

11. V § 10 se na konci textu odstavce 5 doplňují slova „a musí zajistit jejich uchovávání“.

12. V § 12 odst. 4 se slova „srovnatelnou znalostí technologie navštíveného“ nahrazují slovy „znalostí systémů, konstrukcí a komponent v navštíveném“.

13. V § 12 odst. 5 se za slovo „organizační“ vkládají slova „a technická“.

14. V § 13 odst. 1 se slovo „monitorování“ nahrazuje slovem „sledování“.

15. V § 13 odst. 2 se slova „systémem detekujícím jejich narušení, systémem průmyslové televize se záznamem a mechanickými zábrannými prostředky, které musí zabraňovat přistání prostředků pro vzdušnou přepravu fyzických osob, předmětů a materiálu podle parametrů, které jsou zahrnuty v projektové základní hrozbě.“ zrušují a na konci textu odstavce se doplňují písmena a) až c), která znějí:

    „a) systémem detekujícím její narušení prostředky pro vzdušnou přepravu fyzických osob, předmětů a materiálu podle parametrů, které jsou zahrnuty v projektové základní hrozbě,

    b) kamerovým systémem se záznamem a

    c) mechanickými zábrannými prostředky, které musí zpomalovat postup útočníka ze střechy do budovy.“.

16. V § 13 odst. 3 se slovo „a“ nahrazuje slovem „nebo“ a na konci odstavce se doplňují slova „a systémem detekujícím narušení“.

17. V § 13 odst. 4 se za slovo „narušení,“ vkládá slovo „kamerovým“, slovo „monitorování“ se nahrazuje slovem „sledování“ a slova „průmyslové televize“ a věta druhá se zrušují.

18. V § 18 odst. 1 se za slovo „linkami“ vkládá slovo „přímo“, na konci odstavce se doplňují slova „Technický systém fyzické ochrany smí jednosměrně a způsobem bránícím neoprávněným činnostem získávat informace z informačních systémů v areálu jaderného zařízení, které jsou určeny“ a doplňují se písmena a) až c), která znějí:

    „a) k řízení prací na jaderném zařízení,

    b) ke správě oprávnění vstupů do tohoto jaderného zařízení, nebo

    c) ke sledování a evidenci kvalifikací osob vstupujících do areálu jaderného zařízení nebo se v něm pohybujících.“.

19. V § 18 odst. 4 se slova „musí sloužit výhradně pro účely zajištění fyzické ochrany a“ nahrazují slovem „smí“ a za slovo „povolení“ se vkládají slova „za účelem zajištění fyzické ochrany, zvládání radiační mimořádné události, jaderné bezpečnosti a radiační ochrany“.

20. V § 19 odst. 1 se slova „jeho neoprávněnému použití“ nahrazují slovy „narušení jeho bezpečnosti“ a za slovo „hloubky“ se vkládají slova „ , a to prostřednictvím začlenění počítačových systémů do úrovní se stejnou mírou zabezpečení v každé úrovni“.

21. V § 19 odst. 2 se slova „k zajištění“ nahrazují slovem „zajišťující“.

22. V § 19 odst. 3 se slovo „administrativní“ nahrazuje slovem „organizační“.

23. V § 19 odst. 3 a v § 28 odst. 1 písm. h) se slovo „administrativních“ nahrazuje slovem „organizačních“.

24. V § 19 odst. 4 se za slovo „pravidelného“ vkládá slovo „bezpečnostního“.

25. V § 19 se doplňuje odstavec 5, který zní:

„(5) Základní požadavky na zabezpečení počítačových systémů a požadavky na členění zabezpečení počítačových systémů do jednotlivých úrovní podle odstavce 1 stanoví příloha č. 2 k této vyhlášce. V případě, že držitel povolení naplnil požadavky na zavádění bezpečnostních opatření pro kritickou infrastrukturu podle právního předpisu upravujícího kybernetickou bezpečnost, a tyto požadavky odpovídají požadavkům uvedeným v této vyhlášce, má se za to, že držitel povolení naplnil požadavky této vyhlášky.“.

26. V § 20 odstavec 1 zní:

„(1) Od počátku stavebních prací na základech objektů s vlivem na jadernou bezpečnost, radiační ochranu, zvládání radiační mimořádné události nebo zabezpečení musí být staveniště jaderného zařízení ve výstavbě oploceno a musí být zajištěna jeho fyzická ostraha, kontrola vstupu fyzických osob a kontrola vjezdu dopravních prostředků. Hranicí staveniště jaderného zařízení ve výstavbě musí být plot vysoký alespoň 2,5 m.“.

27. V § 28 odst. 1 se na konci písmene h) slovo „a“ nahrazuje čárkou.

28. V § 28 se na konci odstavce 1 tečka nahrazuje slovem „a“ a doplňuje se písmeno j), které zní:

„j) předběžný návrh zajištění počítačového zabezpečení v oblasti řízení jaderné bezpečnosti, evidence jaderného materiálu, fyzické ochrany a zvládání radiační mimořádné události proti jejich úmyslnému zneužití, který obsahuje kapitoly podle přílohy č. 2 k této vyhlášce.“.

29. V § 28 odst. 2 se na konci písmene k) slovo „a“ nahrazuje čárkou.

30. V § 28 se na konci odstavce 2 tečka nahrazuje slovem „a“ a doplňuje se písmeno m), které zní:

„m) návrh zajištění počítačového zabezpečení v oblasti řízení jaderné bezpečnosti, evidence jaderného materiálu, fyzické ochrany a zvládání radiační mimořádné události proti jejich úmyslnému zneužití, který obsahuje kapitoly podle přílohy č. 2 k této vyhlášce.“.

31. V § 28 odst. 3 písm. d) se za slovo „zkoušek“ vkládá slovo „kamerového“ a slova „průmyslové televize“ se zrušují.

32. V § 28 odst. 3 písm. e) se bod 3 zrušuje.

Dosavadní body 4 až 10 se označují jako body 3 až 9.

33. V § 28 odst. 3 se na konci písmene i) slovo „a“ nahrazuje čárkou.

34. V § 28 se na konci odstavce 3 tečka nahrazuje slovem „a“ a doplňuje se písmeno k), které zní:

„k) plán zajištění počítačového zabezpečení v oblasti řízení jaderné bezpečnosti, evidence jaderného materiálu, fyzické ochrany a zvládání radiační mimořádné události proti jejich úmyslnému zneužití, který obsahuje kapitoly podle přílohy č. 2 k této vyhlášce.“.

35. Za část pátou se vkládá nová část šestá, která včetně nadpisu zní:

# „ČÁST ŠESTÁ
## KULTURA ZABEZPEČENÍ

### § 28a

(1) V rámci zavedení, trvalého rozvíjení a udržování kultury zabezpečení musí být

a) předem určena strategie pro její zavedení,

b) určena osoba, která bude odpovědná za zajištění kultury zabezpečení jako její koordinátor,

c) popsán způsob, jak bude provedeno zavedení a následné trvalé rozvíjení a udržování kultury zabezpečení, a

d) prováděno pravidelné hodnocení úrovně kultury zabezpečení.

(2) V rámci provádění zabezpečení je nutno provádět školení a výcvik kultury zabezpečení u všech pracovníků a jiných osob, které se podílejí na zabezpečení.

(3) V rámci provádění zabezpečení je nutno vypracovat a přijmout plán kultury zabezpečení, jehož obsah stanoví příloha č. 3 k této vyhlášce, který bude směřovat k zavedení, trvalému rozvíjení a udržování kultury zabezpečení v rámci organizace, mezi všemi jejími organizačními jednotkami, pracovníky a jinými osobami, které se podílejí na zabezpečení. Plán kultury zabezpečení musí být předložen Úřadu alespoň 90 dnů před zahájením vykonávání činnosti na základě povolení podle § 9 odst. 1 písm. b) až e) atomového zákona.

(4) V rámci provádění zabezpečení je nutno přidělit lidské a finanční zdroje pro zavedení a naplňování plánu kultury zabezpečení a jeho plnění průběžně kontrolovat.

(5) Koordinátor kultury zabezpečení musí dohlížet na plnění a výsledky opatření podle plánu kultury zabezpečení.

(6) Na základě výsledků pravidelného hodnocení úrovně kultury zabezpečení musí dojít, je-li to nezbytné, k

a) aktualizaci plánu kultury zabezpečení a

b) stanovení opatření k posílení kultury zabezpečení.

(7) Aktualizace plánu kultury zabezpečení musí být do 30 dnů oznámena Úřadu.

### § 28b

V rámci provádění zabezpečení je nutno zajistit, aby se všichni pracovníci a jiné osoby, kteří se podílejí na zabezpečení, účastnili zvyšování kultury zabezpečení těmito opatřeními:

a) ochranou utajovaných informací a majetku,

b) zvyšováním povědomí o skutečné hrozbě a významu zabezpečení,

c) splněním požadovaných školicích a výcvikových aktivit v oblasti zabezpečení a poskytnutím zpětné vazby hodnotící jejich přínos a efektivitu,

d) plněním organizačních a technických opatření k provádění zabezpečení a v případě potřeby návrhem jejich změny,

e) zvyšováním znalosti pravidel zabezpečení a kultury zabezpečení,
f) dodržováním pravidel v oblasti kultury zabezpečení,
g) hlášením neobvyklé události nebo situace týkající se zabezpečení,
h) poskytováním pomoci vedoucím pracovníkům v jejich úsilí o vytvoření pracovního prostředí, které podporuje zvyšování kultury zabezpečení,
i) pravidelným poskytováním zpětné vazby vedoucím pracovníkům a koordinátorovi kultury zabezpečení ve věci efektivity plánování, výcviku a spokojenosti s pracovními podmínkami,
j) dotazováním na neobvyklou událost jiného pracovníka nebo jiné osoby, která se podílí na zabezpečení, a
k) pozitivní motivací a povzbuzováním kladného chování v oblasti zabezpečení u ostatních.“.

Dosavadní část šestá se označuje jako část sedmá.

36. Dosavadní příloha se označuje jako příloha č. 1 a doplňují se přílohy č. 2 a 3, které včetně nadpisů znějí:

**„Příloha č. 2**

## POŽADAVKY NA ZABEZPEČENÍ POČÍTAČOVÝCH SYSTÉMŮ V RÁMCI ÚROVNÍ

Bezpečnostní úrovně zabezpečení počítačových systémů jsou v souladu s principem ochrany do hloubky a odstupňovaným přístupem členěny alespoň do pěti úrovní s tím, že Úroveň 1 je úroveň s nejvyšší mírou zabezpečení, následovně:

Úroveň 1 - důležité ochranné a bezpečnostní systémy,

Úroveň 2 - řídicí systémy, další ochranné a bezpečnostní systémy,

Úroveň 3 - podpůrné informační systémy,

Úroveň 4 – komunikační a nadblokové informační systémy,

Úroveň 5 - kancelářské systémy.

**Základní požadavky na zabezpečení počítačových systémů**

a) Technická, fyzická, personální a organizační opatření pro zabezpečení počítačových systémů musí být navržena a realizována systematicky a v souladu s platnými procesy a postupy.
b) Postupy a obvyklá praxe musí být definovány pro každou úroveň zabezpečení počítačových systémů.
c) Pracovníci musí postupovat dle platných postupů a procedur zabezpečení.
d) Pracovníci s právem přístupu k systémům musí být dostatečně vzdělaní, trénovaní a v případě, kdy je to právními předpisy vyžadováno, bezpečnostně způsobilí.
e) Pracovníci smí mít přístup pouze k těm funkcím počítačových systémů, které potřebují ke své práci.
f) Funkcionalita a rozhraní systémů musí být omezeny za účelem snížení celkové zranitelnosti.
g) Přístupová oprávnění musí být řízena, pravidelně kontrolována a ověřována.
h) Počítačové systémy musí být chráněny před škodlivým kódem a jeho šířením.
i) Přístupy do počítačového systému včetně neoprávněných přístupů musí být zaznamenávány, sledovány a zabezpečeny.
j) Poruchovost počítačového systému musí být nepřetržitě sledována a musí být předem připravena nápravná technická opatření.
k) Efektivita, přiměřenost organizačních a technických opatření sloužících k zabezpečení počítačového systému a zranitelnost počítačového systému musí být pravidelně hodnoceny.
l) Přenosné elektronické zařízení umožňující ovlivnit zpracování informací a zabránit nebo narušit plnění bezpečnostní funkce systému, konstrukce nebo komponenty (dále jen „přenosné elektronické zařízení“) musí být kontrolováno v souladu s platným postupem zabezpečení. Na základě provedené studie zranitelnosti musí být regulováno jeho vnášení do vymezených prostorů. Přenosné elektronické zařízení, které neslouží k vykonávání pracovních činností, nesmí být možné spojit se systémem.
m) Opatření k zabezpečení počítačových systémů musí být pravidelně aktualizována vzhledem k případným změnám postupů zabezpečení.
n) Postupy pro zálohování a obnovu dat musí být předem připraveny a zálohy pravidelně testovány.
o) Přenosné elektronické zařízení, které slouží k vykonávání pracovních činností, musí být určeno pro použití pouze v jedné úrovni zabezpečení.
p) Fyzický přístup k jednotlivým částem počítačového systému musí být omezen a řízen podle funkcí těchto částí.
q) Musí být připravena a uplatňována opatření k řízení datových toků mezi jednotlivými úrovněmi zabezpečení.
r) Změnu konfigurace počítačového systému smí provádět pouze schválení a kvalifikovaní pracovníci.

**Předběžný návrh zajištění počítačového zabezpečení v oblasti řízení jaderné bezpečnosti, evidence jaderného materiálu, fyzické ochrany a zvládání radiační mimořádné události proti jejich úmyslnému zneužití [§ 28 odst. 1 písm. j)], návrh zajištění počítačového zabezpečení v oblasti řízení jaderné bezpečnosti, evidence jaderného materiálu, fyzické ochrany a zvládání radiační mimořádné události proti jejich úmyslnému zneužití [§ 28 odst. 2 písm. m)] a plán zajištění počítačového zabezpečení v oblasti řízení jaderné bezpečnosti, evidence jaderného materiálu, fyzické ochrany a zvládání radiační mimořádné události proti jejich úmyslnému zneužití [§ 28 odst. 3 písm. k)] obsahují následující kapitoly:**

a) Organizační uspořádání a stanovení odpovědnosti
   1. organizační struktura,
   2. stanovení odpovědnosti osob a systému hlášení,
   3. systém pravidelného přezkoumávání a schvalovací postupy,
   4. vzájemná spolupráce s dalšími oblastmi jako jsou lidské zdroje, výkon citlivých činností, fyzická ochrana a odborná příprava.

b) Hrozba, zranitelnost a řízení shody
   1. systém hodnocení rizika, stanovení a zařazení počítačových systémů do jednotlivých úrovní,
   2. stanovení četnosti hodnocení plánu zajištění počítačového zabezpečení,
   3. postupy provedení sebehodnocení,
   4. popis auditního hodnocení a odstranění zjištěných nedostatků,
   5. hodnocení shody s platnými právními předpisy.

c) Návrh počítačového zabezpečení a jeho řízení
   1. základy architektury počítačového zabezpečení včetně stanovení jednotlivých úrovní zabezpečení počítačových systémů,
   2. přijatá opatření počítačového zabezpečení na každé úrovni zabezpečení počítačových systémů,
   3. určení požadavků počítačového zabezpečení pro dodavatele včetně požadavků na dodavatelskou údržbu,
   4. posouzení opatření počítačového zabezpečení v rámci životního cyklu jaderného zařízení.

d) Řízení počítačového systému
   1. vlastnosti počítačových systémů, jejich identifikace, úroveň, umístění a možné dopady v případě protiprávních činností proti nim,
   2. konfigurace zabezpečení systému,
   3. síťový diagram s vyznačením datového toku s vnějším spojením na další počítačové systémy.

e) Postupy zabezpečení
   1. postupy v případě incidentu v oblasti zabezpečení počítačových systémů,
   2. popis systému zálohování dat a jejich obnovení,
   3. popis dodavatelského řetězce,
   4. popis systému řízení přístupu,
   5. popis informačního a komunikačního systému,
   6. popis zabezpečení systému aplikací a platforem,
   7. popis systému sledování včetně systému logování.

f) Personální řízení
   1. ověřování citlivých činností,
   2. provádění profesní přípravy,
   3. provádění systému odborné přípravy a vzdělávání,
   4. hlášení incidentů v oblasti zabezpečení včetně ochrany personálu, který tyto události hlásí,
   5. zrušení oprávnění k přístupu do počítačových systémů v případě ukončení pracovního poměru pracovníka nebo jeho převodu na jinou pozici.

**Příloha č. 3**

## OBSAH PLÁNU KULTURY ZABEZPEČENÍ

Plán kultury zabezpečení obsahuje následující informace:

a) určení cílů pro zavedení, trvalé rozvíjení a udržování úrovně zajištění kultury zabezpečení,
b) popis pravidelného hodnocení úrovně kultury zabezpečení,
c) popis školení a výcviku kultury zabezpečení,
d) popis opatření přijatých k dosažení stanovených cílů,
e) určení osob odpovědných za plnění opatření,
f) časový rámec pro plnění opatření,
g) určení zdrojů pro plnění opatření,
h) překážky při plnění opatření,
i) určení postupu pro plnění opatření,
j) očekávané výsledky opatření.“.

## Čl. II

## Přechodná ustanovení

1. Každý, kdo provádí zabezpečení, je povinen vypracovat a přijmout plán kultury zabezpečení podle § 28a odst. 4 vyhlášky č. 361/2016 Sb., ve znění účinném ode dne nabytí účinnosti této vyhlášky, do 1 roku ode dne nabytí účinnosti této vyhlášky.
2. Držitel povolení podle § 9 odst. 1 písm. a) až e) atomového zákona je povinen uvést analýzu potřeb a možnosti zajištění fyzické ochrany, předběžný plán zajištění fyzické ochrany a plán zajištění fyzické ochrany do souladu s požadavky na tyto dokumenty stanovenými vyhláškou č. 361/2016 Sb., ve znění účinném ode dne nabytí účinnosti této vyhlášky, do 1 roku ode dne nabytí účinnosti této vyhlášky.

## Čl. III

## Účinnost

Tato vyhláška nabývá účinnosti dnem 1. července 2025.

Předsedkyně:
Ing. Drábová, Ph.D., v. r.

ISSN 3029-5092

Vydavatel: Ministerstvo vnitra, Nad Štolou 3, poštovní schránka 21, 170 34 Praha 7 • **Redakce Sbírky zákonů a mezinárodních smluv**: Ministerstvo vnitra, nám. Hrdinů 1634/3, poštovní schránka 155/SB, 140 21, Praha 4, telefon: 974 817 289, e-mail: sbirka@mvcr.cz • Sazba: Tiskárna Ministerstva vnitra, Bartůňkova 1159/4, poštovní schránka 10, 149 00 Praha 11-Chodov • **Právně závazná elektronická verze Sbírky zákonů a mezinárodních smluv je k dispozici na www.e-sbirka.cz** • Tištěnou verzi částky Sbírky zákonů a mezinárodních smluv lze objednat u Tiskárny Ministerstva vnitra, telefon: 974 887 312, e-mail: info@tmv.cz, www.tmv.cz • Předplatné je od 1. 1. 2024 ukončeno.