PORTÁL NÚKIB

Řízení bezpečnostní politiky a bezpečnostní dokumentace

Režim nižších povinností

TLP:CLEAR

31. března 2026

Verze 1.0

Národní úřad pro kybernetickou a informační bezpečnost

Obsah

1 Úvod

Subjekty spadající pod regulaci zákona č. 264/2025 Sb. o kybernetické bezpečnosti (dále jen „zákon“) mají ve vztahu k řízení kybernetické bezpečnosti regulované služby povinnost stanovit bezpečnostní politiky a vést bezpečnostní dokumentaci k relevantním bezpečnostním opatřením uvedeným ve vyhlášce č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností (dále jen „vyhláška č. 410/2025 Sb.“). Cílem tohoto opatření je, aby všechna pravidla, metody, kritéria a postupy byly aktuální, zdokumentované a schválené, tedy i vymahatelné.

Pokud máte jakékoliv další otázky, podívejte se na www.portal.nukib.gov.cz nebo nám napište na regulace@nukib.gov.cz.

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti publikované verze dokumentu.

1.1 Jak pracovat s podpůrným materiálem

V tomto materiálu je uvedena možná struktura bezpečnostních politik a bezpečnostní dokumentace, která slouží jako vodítko při implementaci tohoto požadavku pro poskytovatele regulované služby v režimu nižších povinností, včetně bližších popisů dokumentů. Materiál sumarizuje a strukturalizuje požadavky vyhlášky č. 410/2025 Sb. na řídicí dokumentaci, ale také doplňuje některé další dokumenty sloužící pro usnadnění řízení kybernetické bezpečnosti.

> ***Obsah a strukturu bezpečnostní politiky a bezpečnostní dokumentace je potřeba přizpůsobit procesům a potřebám konkrétní organizace.***
>
> ***Struktura uvedená v tomto materiálu slouží pouze jako příklad. To znamená, že z uvedených oblastí nemusí být pro každou organizaci vždy všechny relevantní, nebo naopak pro ni mohou být relevantní i takové oblasti, které nejsou v tomto materiálu uvedeny. Proto tento materiál neslouží jako kontrolní seznam pro ověřování plnění povinností stanovených zákonem***

Z pohledu plnění požadavků vyhlášek o bezpečnostních opatřeních nezáleží na tom, v kolika dokumentech budou dané oblasti popsány a jak budou dokumenty pojmenovány. Důležitá je obsahová úplnost a zasazení do řídicí dokumentace dané organizace. Přesná shoda s tímto podpůrným materiálem tudíž není nezbytná.

2 Seznam použitých zkratek a pojmů

BYOD	Bring Your Own Device (Přines si vlastní zařízení)
KBI	kybernetický bezpečnostní incident
KBU	kybernetická bezpečnostní událost
SLA	Service Level Agreement (smlouva o úrovni služeb)
Vyhláška č. 410/2025 Sb.	Vyhláška č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností
Zákon	Zákon č. 264/2025 Sb. o kybernetické bezpečnosti

Pro potřeby tohoto dokumentu jsou definovány následující pojmy:

- **Bezpečnostní politikou** se rozumí soubor základních pravidel, praktik, kritérií, postupů a odpovědností, které stanovují způsob řízení kybernetické bezpečnosti a zajišťování bezpečnosti informací regulované služby. Bezpečnostní politiky mohou být dále rozpracovány a specifikovány v bezpečnostní dokumentaci. Cílem je, aby všechna pravidla, praktiky, kritéria a postupy byly aktuální, zdokumentované a schválené, tedy i vymahatelné.
- **Bezpečnostní dokumentace** specifikuje konkrétní postupy a procesy definované v bezpečnostních politikách a slouží jako praktický návod pro zaměstnance. Jedná se například o metodiku pro určování a hodnocení aktiv a rizik, plány kontinuity činností, plány obnovy, přehled síťové komunikační infrastruktury.

3 Bezpečnostní politika a bezpečnostní dokumentace

Požadavky na bezpečnostní politiku a bezpečnostní dokumentaci se odvíjí od režimu povinností, do kterého poskytovatel regulované služby spadá. U režimu nižších povinností jsou požadavky zredukovány na nezbytné minimum a vychází z obsahu a rozsahu bezpečnostních opatření stanovených vyhláškou č. 410/2025 Sb.

Poskytovatel regulované služby v režimu nižších povinností musí dle § 3 odst. 3 vyhlášky č. 410/2025 Sb. v rámci řízení bezpečnostní politiky a bezpečnostní dokumentace:

a) **Stanovit** bezpečnostní politiku a bezpečnostní dokumentaci k bezpečnostním opatřením požadovaným vyhláškou č. 410/2025 Sb.

b) **Pravidelně přezkoumávat a aktualizovat** pravidla a postupy stanovené v bezpečnostní politice a bezpečnostní dokumentaci.

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

Bezpečnostní politika by měla vymezovat taková pravidla a postupy, které jsou v organizaci již zavedeny nebo jejichž implementace je reálně plánována v dohledném časovém horizontu. **Neměla by obsahovat obecné či deklarativní formulace bez praktického dopadu ani mechanicky přebírat požadavky vyhlášky č. 410/2025 Sb. bez jejich konkretizace.** Naopak by měla z legislativních požadavků systematicky vycházet a převádět je do konkrétního nastavení odpovídajícího prostředí, procesům a možnostem dané organizace.

4 Bezpečnostní politiky

4.1 Politika zajišťování kybernetické bezpečnosti

K čemu slouží:

Jedná se o zastřešující politiku, která ukotvuje řízení kybernetické bezpečnosti v organizaci. Stanovuje pravidla pro určení aktiv spadajících do rozsahu řízení kybernetické bezpečnosti a určuje způsob jejich ochrany a používání. Zároveň definuje minimální technické požadavky na kybernetickou bezpečnost, které musí být naplněny v rámci akvizice, vývoje a údržby těchto aktiv. V neposlední řadě vymezuje povinnosti vrcholného vedení a jeho závazek ke zvyšování úrovně kybernetické bezpečnosti.

Co by měla pokrývat:

- Pravidla pro určení a Evidenci aktiv (5.2).
    - Pravidla a postupy pro určení a evidenci primárních aktiv.
        - Určení a evidence primárních aktiv souvisejících s regulovanou službou.
        - Určení a evidence primárních aktiv nesouvisejících s regulovanou službou.
    - Pravidla a postupy pro určení a evidenci garantů primárních aktiv.
    - Pravidla a postupy pro určení a evidenci vazeb mezi aktivy.
    - Pravidla a postupy pro určení a evidenci podpůrných aktiv.
    - Pravidla a postupy pro určení a evidenci garantů podpůrných aktiv.
- Rozsah a hranice řízení kybernetické bezpečnosti.
- Pravidla pro vedení, aktualizaci a vyhodnocení Přehledu bezpečnostních opatření (5.1).
- Pravidla ochrany a přípustné způsoby používání technických aktiv.
- Bezpečnostní požadavky pro řízení akvizice, vývoje a údržby technických aktiv.
- Pravidla a postupy pro přezkum a aktualizaci bezpečnostních politik a bezpečnostní dokumentace.
- Povinnosti vrcholného vedení v rámci řízení kybernetické bezpečnosti.

4.2 Politika řízení dodavatelů

K čemu slouží:

Politika stanovuje veškerá nezbytná pravidla a postupy související s řízením dodavatelů. Vymezuje požadavky kladené na dodavatele, pravidla jejich výběru a potřebné náležitosti smluv.

Co by měla pokrývat:

- Pravidla pro dodavatele.
- Pravidla a postupy pro výběr dodavatelů.
- Pravidla a postupy pro zohlednění hrozeb a zranitelností spojených s dodavatelem, jeho celkovou kvalitou produktů a postupů v oblasti kybernetické bezpečnosti, včetně postupů bezpečného vývoje.
- Náležitosti smlouvy zohledňující relevantní požadavky na dodavatele z přílohy č. 2 vyhlášky č. 410/2025 Sb.

- Náležitosti smlouvy o úrovni služeb (*SLA*) a způsobu a úrovni realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti.
- Pravidla pro vedení evidence kontaktních údajů dodavatelů pověřených výkonem systémové a technické podpory.

4.3 Politika bezpečnosti lidských zdrojů

K čemu slouží:

Cílem politiky je vymezit systém školení zaměstnanců, tedy stanovit školení kybernetické bezpečnosti, která jsou zaměstnanci povinni absolvovat, a nastavit jejich frekvenci. Politika dále upravuje životní cyklus uživatele, zejména nastavení procesů od jeho nástupu přes změnu pracovní pozice až po ukončení pracovního vztahu. V neposlední řadě stanovuje pravidla chování uživatelů a postupy pro řešení případů jejich porušení.

Co by měla pokrývat:

- Pravidla rozvoje bezpečnostního povědomí.
- Vstupní školení v oblasti kybernetické bezpečnosti.
- Stanovení periody pro pravidelná školení.
- Pravidla evidence přehledů o školeních.
- Pravidla a postupy pro zohlednění relevantních témat kybernetické hygieny uvedených v příloze č. 3 vyhlášky č. 410/2025 Sb. v rámci školení.
- Pravidla a postupy pro zajištění odborných, teoretických i praktických školení administrátorů a osob odpovědných za kybernetickou bezpečnost v souladu s jejich pracovní náplní.
- Pravidla pro řešení případů porušení bezpečnostní politiky.
- Pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice.
    - Vrácení svěřených aktiv a odebrání práv při ukončení pracovního vztahu.
    - Změna přístupových oprávnění při změně pracovní pozice.
    - Předání odpovědností při změně pracovní pozice nebo ukončení pracovního vztahu s administrátory nebo osobou odpovědnou za kybernetickou bezpečnost.

4.4 Politika bezpečného chování uživatelů

K čemu slouží:

Politika slouží k nastavení všech bezpečnostních pravidel, kterými se musí osoby přistupující k aktivům regulované služby řídit.

Co by měla pokrývat:

- Pravidla základní kybernetické hygieny zohledňující témata uvedená v příloze č. 3 vyhlášky č. 410/2025 Sb.
- Pravidla pro tvorbu a používání hesel účtů
    - uživatelů,
    - administrátorů a
    - technických aktiv.

- Pravidla a postupy pro bezpečné nakládání s technickými aktivy, včetně vyměnitelných zařízení a datových nosičů.
- Pravidla a postupy pro bezpečný vzdálený přístup.
- Pravidla a postupy pro oznamování neobvyklého chování technických aktiv a podezření na jakékoliv zranitelnosti.
- Způsoby vynucování bezpečnostních politik.

4.5 Politika řízení kontinuity činností

K čemu slouží:

Politika slouží k jasnému organizačnímu zajištění kontinuity činností a dostupnosti regulované služby. Stanovuje procesy pro zvládání krizových situací a vymezuje práva a povinnosti odpovědných osob, komunikační matice a postupy pro obnovení chodu systému, které jsou detailněji rozpracovány v Plánu obnovy (5.4).

Co by měla pokrývat:

- Priority obnovy primárních aktiv.
- Prioritizace technických aktiv a pořadí a postupy jejich obnovy včetně určení odpovědností.
- Komunikační matice s klíčovými osobami pro jednotlivé činnosti.
- Postupy pro spuštění a ukončení chodu systému, pro restart nebo obnovení chodu systému po selhání a pro ošetření chybových stavů nebo mimořádných jevů.
- Pravidla a postupy pro zálohování.

4.6 Politika řízení přístupu

K čemu slouží:

Politika stanovuje pravidla a postupy pro řízení identit a jejich oprávnění v rámci přístupu k aktivům regulované služby. Nastavuje procesy pro celý životní cyklus identit od jejich založení, přes změny oprávnění nebo řešení nestandardních situací, až po jejich zánik.

Co by měla pokrývat:

- Pravidla a postupy pro práci s nástrojem sloužícím pro správu a ověření identit a s nástrojem řídícím přístupová práva a oprávnění a definování povinností odpovědných osob.
- Pravidla a postupy pro řízení identifikátorů, přístupových práv a oprávnění.
- Pravidla a postupy pro bezpečné používání mobilních zařízení.
- Pravidla, postupy a evidence pro účty sloužící zejména pro případ obnovy po KBI.
- Pravidla pravidelného přezkoumání přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách.
- Pravidla a postupy pro odebrání nebo změnu přístupových oprávnění.
- Pravidla a postupy pro zajištění důvěrnosti při vytváření výchozích autentizačních údajů a při obnově přístupu.
- Pravidla a postupy pro využívání administrátorských účtů a technických aktiv určených zejména pro případ obnovy po KBI.

- Pravidla a postupy pro zajištění bezpečnosti zařízení, která poskytovatel regulované služby nemá ve své správě (*BYOD*).

4.7 Politika fyzické bezpečnosti

K čemu slouží:

Politika slouží k nastavení pravidel pro zajištění fyzické bezpečnosti za účelem ochrany aktiv regulované služby.

Co by měla pokrývat:

- Pravidla a postupy pro ochranu fyzického bezpečnostního perimetru objektů a umístěných aktiv regulované služby.
- Pravidla a postupy pro kontrolu a evidenci vstupu osob za účelem ochrany aktiv regulované služby.

4.8 Politika detekce KBU a řešení KBI

K čemu slouží:

Politika slouží k nastavení pravidel pro detekci a zvládání KBI.

Co by měla pokrývat:

- Definování KBU a KBI.
- Pravidla a postupy pro nasazení, nastavení, užívání a aktualizaci nástroje pro nepřetržitou a automatickou ochranu před škodlivým kódem, včetně definování odpovědnosti za jednotlivé činnosti.
- Pravidla a postupy pro detekci KBU.
- Pravidla a postupy pro zaznamenávání KBU a relevantních provozních událostí.
- Pravidla a postupy pro bezpečné uchovávání a retenci KBU a relevantních provozních událostí.
- Pravidla a postupy pro řešení KBI.
- Pravidla a postupy pro identifikaci a klasifikaci KBI s významným dopadem, na které navazuje Metodika pro posuzování KBU a KBI (5.5).
- Pravidla a postupy pro hlášení KBI s významným dopadem, na které navazuje Závěrečná zpráva o vyřešení KBI s významným dopadem (5.6).

4.9 Politika bezpečnosti komunikační sítě

K čemu slouží:

Politika stanovuje pravidla pro zabezpečení komunikační sítě. Vymezuje požadavky na nastavení sítě, zejména v oblasti segmentace sítě a řízení komunikace v rámci interního prostředí a na perimetru sítě. Rovněž se věnuje problematice vzdáleného přístupu a vzdálené správy technických aktiv.

Co by měla pokrývat:

- Pravidla a postupy pro zajištění segmentace komunikační sítě a oddělení jednotlivých prostředí.
- Pravidla a postupy pro zajištění bezpečného provozu komunikační sítě a omezení komunikace na perimetru komunikační sítě.
- Pravidla a postupy pro řízení vzdáleného přístupu ke komunikační síti, a to včetně vzdáleného přístupu dodavateli nebo jinými osobami.
- Pravidla a postupy pro vzdálenou správu technických aktiv, a to včetně vzdálené správy technických aktiv dodavatelem nebo jinými osobami.
- Pravidla využívání kryptografických algoritmů.
- Určení práv a povinností za účelem bezpečného provozu komunikační sítě.
- Pravidla pro vedení přehledu o uživatelích a administrátorech, kteří využívají vzdálené připojení nebo vzdálenou správu.

4.10 Politika aplikační bezpečnosti

K čemu slouží:

Politika se primárně zaměřuje na řízení bezpečnostních aktualizací a zranitelností technických aktiv. Vymezuje postupy pro celý životní cyklus zranitelností od jejich identifikace, například prostřednictvím pravidelného skenování, až po jejich nápravu. Současně stanovuje postupy pro řešení neopravitelných zranitelností u již nepodporovaných technických aktiv.

Co by měla pokrývat:

- Pravidla a postupy pro nasazení a aplikování aktualizací vydaných pro technická aktiva.
- Pravidla a postupy pro Evidenci technických aktiv, která již nejsou výrobcem, dodavatelem nebo jinou osobou podporována (5.7) a zajištění ochrany těchto aktiv.
- Pravidla a postupy pro provádění pravidelného skenování zranitelností a práci s nálezy.

5 Obsah bezpečnostní dokumentace

5.1 Přehled bezpečnostních opatření

K čemu slouží:

Slouží jako přehled stavu zavedení všech bezpečnostních opatření uvedených ve vyhlášce č. 410/2025 Sb.

Co by měl pokrývat:

- Přehled všech bezpečnostních opatření, která byla zavedena, včetně popisu jejich zavedení.
- Přehled všech bezpečnostních opatření, která budou zavedena.
  - Termíny pro jejich zavedení.
  - Priority jejich zavedení.
  - Určení osoby odpovědné za jejich zavedení.
- Přehled všech bezpečnostních opatření, která nebyla zavedena, včetně odůvodnění jejich nezavedení.

5.2 Evidence aktiv

K čemu slouží:

Dokument slouží k mapování primárních a podpůrných aktiv, a tím k vymezení stanoveného rozsahu řízení kybernetické bezpečnosti.

Co by měla pokrývat:

- Přehled všech primárních aktiv.
  - Určení a popis primárních aktiv souvisejících s regulovanou službou.
  - Určení a popis primárních aktiv nesouvisejících s regulovanou službou.
  - Určení garantů primárních aktiv.
  - Stanovení priority obnovy primárních aktiv.
- Přehled podpůrných aktiv.
  - Určení a popis podpůrných aktiv.
  - Určení garantů podpůrných aktiv.
- Určení vazeb mezi primárními a podpůrnými aktivy.

5.3 Přehled o provedených školení

K čemu slouží:

Přehled slouží pro zajištění přehlednosti a průkaznosti ohledně absolvování školení a poučení jednotlivých osob.

Co by měl pokrývat:

- Obsah daného školení.
- Seznam osob, které jej absolvovaly, včetně jejich podpisů.
- Datum konání školení.

- Přehledy poučení vrcholného vedení o jeho povinnostech a o bezpečnostní politice.
- Přehledy vstupních školení v oblasti kybernetické bezpečnosti.
- Přehledy pravidelných školení v oblasti kybernetické bezpečnosti.
- Přehledy odborných školení administrátorů a osoby pověřené kybernetickou bezpečností.

5.4 Plán obnovy

K čemu slouží:

Plán obnovy slouží jako průvodce pro obnovení poskytování regulované.

Co by měl pokrývat:

- Jednoznačné postupy obnovy pro různé scénáře nedostupnosti regulované služby.
- Povinnosti a odpovědnosti jednotlivých relevantních osob.
- Kontaktní matice na tyto osoby.

5.5 Metodika pro posuzování KBU a KBI

K čemu slouží:

Metodika stanovuje kritéria a postup pro posouzení, zda se jedná o KBI s významným dopadem, který je poskytovatel regulované služby povinen oznámit Národnímu CERT. Podrobnosti naleznete v materiálu Významnost incidentu v režimu nižších povinností.

Co by měla pokrývat:

- Stanovení únosné míry újmy způsobené KBI.
- Oblasti pro posouzení významnosti KBI.
- Podmínky určující dopad KBI na poskytování regulované služby jako významný.
- Povinnosti a odpovědnosti jednotlivých relevantních osob.

5.6 Závěrečná zpráva o vyřešení KBI s významným dopadem

K čemu slouží:

Tato zpráva slouží k zaznamenání vyřešeného KBI. V případě KBI s významným dopadem je poskytovatel regulované služby povinen tuto zprávu vypracovat a předložit Národnímu CERT.

Co by měla pokrývat:

- Datum a čas zjištění KBI.
- Rozsah zasažených aktiv a jejich popis.
- Stav řešení KBI.
- Popis příčiny vzniku KBI, pokud je známa.
- Popis průběhu KBI a indikátory kompromitace.
- Postup řešení KBI.
- Projevy KBI, jeho dopad a vzniklé škody.
- Zdroje potřebné k obnově regulované služby.
- Lokace KBI.

- Citlivost zasažených dat a posouzení přeshraničního dopadu.
- Výčet subjektů, které byly KBI zasaženy.

5.7 Evidence technických aktiv, která již nejsou podporována

K čemu slouží:

Evidence slouží k vedení přehledu všech technických aktiv, která již nejsou výrobcem podporována. Obsahuje jejich úplný seznam a u každého aktiva veškeré nezbytné informace, zejména zavedená bezpečnostní opatření, která snižují nebo zamezují riziku zneužití jejich neošetřených zranitelností.

Co by měla pokrývat:

- Popis těchto technických aktiv.
- Garanti těchto technických aktiv.
- Způsoby zavedení bezpečnostních opatření, která zaručí obdobnou nebo vyšší úroveň bezpečnosti těchto technických aktiv.

5.8 Přehled síťové komunikační infrastruktury

K čemu slouží:

Tento přehled slouží k přehledné vizualizaci interní komunikační sítě a infrastruktury. Měl by obsahovat názorný diagram zohledňující úrovně L1, L2 a L3 ISO/OSI modelu a dále také seznam jednotlivých VLAN včetně jejich názvů a využití.

Co by měl pokrývat:

- Schéma a popis topologie interní komunikační sítě a infrastruktury.
- Segmentaci komunikační sítě a infrastruktury.
- Přehled bezpečnostních prvků v síťové infrastruktuře.

5.9 Kontakt na osoby pověřené technickou a systémovou podporou

K čemu slouží:

Tyto kontakty slouží pro rychlé a efektivní získání technické podpory a vyřešení nedostupnosti regulované služby.

Co by měl pokrývat:

- Kontakty na jednotlivé relevantní osoby, popř. i záložní kontakty.

6 Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol. Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
TLP:RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
TLP:AMBER+STRICT	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:AMBER	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:GREEN	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
TLP:CLEAR	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Verze dokumentu			
datum	**verze**	**změněno**	**popis změny**
31. března 2026	1.0	Odbor kontroly	Vytvoření dokumentu