PORTÁL NÚKIB

Řízení bezpečnostní politiky a bezpečnostní dokumentace

Režim vyšších 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. 409/2025 Sb. o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (dále jen „vyhláška č. 409/2025 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 vyšších povinností, včetně bližších popisů dokumentů. Materiál sumarizuje a strukturalizuje požadavky vyhlášky č. 409/2025 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 vyhlášky č. 409/2025 Sb. 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)
ISMS	Systém řízení bezpečnosti informací
KBI	kybernetický bezpečnostní incident
KBU	kybernetická bezpečnostní událost
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OT	Operational Technology
SLA	Service Level Agreement (smlouva o úrovni služeb)
VLAN	Virtual Local Area Network
Vyhláška č. 409/2025 Sb.	Vyhláška č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších 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 nebo provozní 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 např. o metodiku pro určování a hodnocení aktiv a rizik, plány kontinuity činností, plány obnovy, přehled síťové komunikační infrastruktury apod.
- **Provozní dokumentace** je soubor dokumentů, které pracují s reálnými daty z provozu regulované služby. Jedná se např. o provozní deník, záznamy o stavech nebo kontrolách, záznam o změnách apod.

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 vyšších povinností jsou požadavky na bezpečnostní politiku a bezpečnostní dokumentaci komplexnější a vychází z obsahu a rozsahu bezpečnostních opatření stanovených vyhláškou č. 409/2025 Sb.

Poskytovatel regulované služby v režimu vyšších povinností musí dle § 6 vyhlášky č. 409/2025 Sb. v rámci řízení bezpečnostní politiky a bezpečnostní dokumentace:

(1) **Stanovit** bezpečnostní politiku ve vztahu k řízení kybernetické bezpečnosti **a vést bezpečnostní politiku a bezpečnostní dokumentaci** k relevantním bezpečnostním opatřením uvedeným v § 3 až 27 vyhlášky č. 409/2025 Sb.

(2) **Dodržovat pravidla a postupy** stanovené v bezpečnostní politice a bezpečnostní dokumentaci.
(3) **Pravidelně přezkoumávat** bezpečnostní politiku a bezpečnostní dokumentaci, zajistit jejich **aktuálnost** a **zohlednit jejich relevantní oblasti** v provozní dokumentaci, pravidlech a postupech.
(4) **Určit osobu odpovědnou** za pravidelný přezkum a aktualizaci bezpečnostní politiky a bezpečnostní dokumentace.
(5) Řídit bezpečnostní politiku a bezpečnostní dokumentaci tak, aby **byly**
   a) **dostupné** v elektronické nebo listinné podobě,
   b) **dotčené osoby** v rámci povinné osoby **informovány** o právech, povinnostech a postupech v nich obsažených,
   c) přiměřeně dostupné dotčeným stranám,
   d) **chráněny** z pohledu důvěrnosti, integrity a dostupnosti a
   e) informace v nich obsažené **úplné, čitelné**, snadno **identifikovatelné** a **vyhledatelné**.

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. 409/2025 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 systému řízení bezpečnosti informací

K čemu slouží:

Jedná se o zastřešující politiku, která stanovuje systém řízení bezpečnosti informací (dále jen „ISMS“) v organizaci. Měla by stanovit cíle, kterých chce organizace zavedením ISMS dosáhnout, a které vychází z jejích aktuálních bezpečnostních potřeb. Dále by měla určit hranice ISMS formou stanovení rozsahu řízení kybernetické bezpečnosti, ten musí zahrnovat všechna aktiva související s poskytováním regulované služby. Tím dochází k vymezení aktiv, u kterých je nutné zavádět bezpečnostní opatření. V neposlední řadě by měla politika také určit, jakým způsobem chce organizace stanovených cílů dosáhnout a jakým způsobem bude hodnocena účinnost ISMS. Na tuto politiku navazuje Zpráva o přezkoumání ISMS (5.1).

Co by měla pokrývat:

- Cíle, principy a potřeby ISMS.
- Rozsah a hranice řízení kybernetické bezpečnosti.
- Pravidla a postupy pro plánování, řízení a zaznamenávání činnosti lidských a technických zdrojů ISMS.
- Pravidla a postupy pro vyhodnocení účinnosti a přezkoumání ISMS.
- Pravidla a postupy pro nápravná opatření a zlepšování ISMS.

- Závazek vrcholného vedení ve vztahu k dosažení cílů ISMS.
- Povinnosti vrcholného vedení v rámci ISMS.

4.2 Politika organizační bezpečnosti

K čemu slouží:

Politika slouží ke zřízení výboru pro řízení kybernetické bezpečnosti a stanovení bezpečnostních rolí požadovaných vyhláškou č. 409/2025 Sb. a definuje, jakým způsobem musí být role odděleny od organizačních celků zajišťujících provoz technických aktiv regulované služby, aby nedocházelo k možnému střetu zájmů mezi provozem a bezpečností. Politika také míří na určení práv a povinností všech uživatelů a administrátorů přistupujících k aktivům regulované služby.

Co by měla pokrývat:

- Zřízení výboru pro řízení kybernetické bezpečnosti a určení jeho členů, práv a povinností.
- Stanovení bezpečnostních rolí a jejich práv a povinností.
- Stanovení práv a povinností uživatelů a administrátorů.
- Požadavky na oddělení výkonu činností jednotlivých bezpečnostních rolí.
- Požadavky na oddělení výkonu bezpečnostních a provozních rolí.

4.3 Politika řízení bezpečnostní politiky a bezpečnostní dokumentace

K čemu slouží:

Politika slouží k nastavení procesů, které zajistí, aby bezpečnostní politiky a bezpečnostní dokumentace byly udržovány v aktuálním, schváleném a účinném stavu. Toho je dosaženo jednoznačným určením osob odpovědných za jejich pravidelný přezkum, aktualizaci a stanovení pravidel a postupů, jak tyto činnosti provádět.

Co by měla pokrývat:

- Určení osoby odpovědné za pravidelný přezkum a aktualizaci bezpečnostních politik a bezpečnostní dokumentace.
- Pravidla a postupy pro přezkum a aktualizaci bezpečnostních politik a bezpečnostní dokumentace.

4.4 Politika řízení aktiv

K čemu slouží:

Politika slouží k nastavení procesů, pravidel, postupů a odpovědností v rámci řízení aktiv. Jinými slovy zajišťuje efektivní nastavení celého životního cyklu aktiv počínaje jejich pořízením, přes užívání nebo správu až po jejich likvidaci. Na tuto politiku navazuje Metodika pro určování a hodnocení aktiv (5.3) a Evidence aktiv (5.4).

Co by měla pokrývat:

- Proces řízení aktiv.
- Odpovědnosti za proces řízení aktiv.
- Pravidla ochrany jednotlivých úrovní aktiv
  - Přípustné způsoby používání aktiv.
  - Pravidla pro manipulaci s aktivy, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv.
  - Pravidla pro klasifikaci informací.
  - Pravidla pro označování aktiv.
  - Pravidla správy výměnných médií.
  - Pravidla pro určení způsobu likvidace informací a dat a jejich kopií a likvidace technických aktiv, která jsou nosiči informací a dat s ohledem na úroveň aktiv.

4.5 Politika řízení rizik

K čemu slouží:

Tato politika slouží k nastavení procesu řízení rizik a stanovení odpovědností v rámci tohoto procesu. Na tuto politiku navazuje Metodika pro určování a hodnocení rizik (5.5).

Co by měla pokrývat:

- Proces řízení rizik.
- Odpovědnosti za proces řízení rizik.

4.6 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, potřebné náležitosti smluv a principy řízení rizik spojených s dodavateli.

Co by měla pokrývat:

- Pravidla pro dodavatele.
- Pravidla a postupy pro výběr dodavatelů.
- Pravidla a principy určování významných dodavatelů.
- Pravidla a postupy pro hodnocení rizik souvisejících s výběrovým řízením u významných dodavatelů.
- Náležitosti smlouvy zohledňující relevantní požadavky na dodavatele plynoucí ze ISMS.
- Náležitosti smlouvy o úrovni služeb (*SLA*) a způsobu a úrovni realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti.
- Pravidla pro provádění kontroly zavedení bezpečnostních opatření u významných dodavatelů.

- Pravidla pro vedení evidence kontaktních údajů dodavatelů pověřených výkonem systémové a technické podpory.
- Pravidla pro eliminaci závislosti na jednom dodavateli (zejména problematika vendor lock-in a exit strategie).

4.7 Politika bezpečnosti lidských zdrojů

K čemu slouží:

Politika slouží k nastavení pravidel a postupů týkajících se vzdělávání zaměstnanců. Určuje požadavky na jejich školení a vzdělávání s cílem neustálého zlepšování jejich bezpečnostního povědomí a bezpečnostních návyků. Na tuto politiku navazuje Plán rozvoje bezpečnostního povědomí (5.10).

Co by měla pokrývat:

- Pravidla a postupy poučení a školení.
- Stanovení lhůt pro pravidelné opakování školení pro uživatele, administrátory, osoby zastávající bezpečnostní role a vrcholné vedení.
- Formy a způsoby hodnocení účinnosti plánu rozvoje bezpečnostního povědomí.
- Pravidla a postupy pro řešení případů porušení bezpečnostní politiky ISMS.
- Pravidla a postupy při ukončení pracovního vztahu nebo změně 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 osobami zastávajícími bezpečnostní role.
- Pravidla a postupy pro kontrolu dodržování bezpečnostních politik.
- Způsob vedení přehledu o školeních.

4.8 Politika bezpečného chování uživatelů a dalších osob

K čemu slouží:

Politika slouží k nastavení všech bezpečnostních pravidel, kterými se musí osoby přistupující k aktivům regulované služby řídit (uživatelé, administrátoři a osoby zastávající bezpečnostní role).

Co by měla pokrývat:

- Pravidla základní kybernetické hygieny.
- Pravidla pro tvorbu a používání hesel
    - uživatelů,
    - administrátorů a
    - technických aktiv.
- Pravidla a postupy pro bezpečné nakládání s technickými aktivy, včetně vyměnitelných zařízení a datových nosičů.
- Pravidla a postupy pro bezpečné nakládání s přístupovými hesly a dalšími autentizačními způsoby.

- Pravidla a postupy pro bezpečné použití elektronické pošty a přístupu na internet.
- Pravidla a postupy pro bezpečný vzdálený přístup.
- Pravidla a postupy pro bezpečné chování na internetu a sociálních sítích.
- Pravidla a postupy pro oznamování neobvyklého chování technických aktiv a podezření na jakékoliv zranitelnosti.

4.9 Politika bezpečného používání mobilních zařízení

K čemu slouží:

Politika slouží k formalizaci organizačních a technických požadavků u mobilních zařízení, jako jsou mobilní telefony, tablety nebo notebooky. Politika by měla kromě pravidel používání techniky zahrnovat také technické požadavky na samotnou techniku, jako je například možnost vzdálené správy zařízení.

Co by měla pokrývat:

- Pravidla a postupy pro bezpečné nakládání a používání mobilních zařízení v interní komunikační síti i mimo ni.
- Pravidla a postupy pro zajištění bezpečnosti zařízení, která poskytovatel regulované služby nemá ve své správě (*BYOD*).

4.10 Politika řízení změn

K čemu slouží:

Politika slouží k nastavení procesu řízení změn tak, aby o nich měl poskytovatel regulované služby adekvátní přehled a mohl účinně vyhodnocovat jejich možné dopady na kybernetickou bezpečnost a určovat významné změny. Politika slouží k nastavení bezpečnostních postupů u významných změn, včetně jejich testování nebo případného navrácení změny do původního stavu.

Co by měla pokrývat:

- Pravidla a postupy pro řízení změn.
- Pravidla a postupy pro určování a schvalování změn, které mají nebo mohou mít vliv na kybernetickou bezpečnost.
- Pravidla, postupy a kritéria pro přezkoumávání dopadů změn za účelem určování významných změn.
- Pravidla a postupy pro hodnocení rizik spojených s významnou změnou a výběr bezpečnostních opatření.
- Pravidla a postupy pro řízení významných změn.
- Způsob vedení evidence významných změn.
- Pravidla a postupy pro testování významných změn před jejich uvedením do provozu, včetně možnosti navrácení do původního stavu (*Rollback*).
- Pravidla a postupy pro rozhodování o provedení penetračního testování.

4.11 Politika akvizice, vývoje a údržby

K čemu slouží:

Politika slouží pro stanovení bezpečnostních požadavků, které je nutné zohledňovat v rámci akvizice, vývoje a údržby technických aktiv.

Co by měla pokrývat:

- Bezpečnostní požadavky pro akvizici, vývoj a údržbu.
- Bezpečnostní požadavky na oddělení provozního, zálohovacího, vývojového, testovacího, administrátorského a jiných specifických prostředí.
- Bezpečnostní požadavky na vícefaktorovou autentizaci.
- Bezpečnostní požadavky na kryptografické algoritmy.
- Bezpečnostní požadavky s ohledem na užití principu nulové důvěry (*Zero Trust*).
- Bezpečnostní požadavky na dostupnost bezpečnostních aktualizací po dobu životního cyklu technických aktiv.
- Bezpečnostní požadavky na řízení zranitelností.
- Pravidla a postupy pro nasazení a údržbu technických aktiv.
- Pravidla a postupy poskytování a nabývání licencí programového vybavení a informací.
    - Pravidla a postupy nasazení a údržby programového vybavení a jeho evidence.
    - Pravidla a postupy pro kontrolu dodržování licenčních podmínek.

4.12 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. Politika by měla zahrnovat všechny druhy identit, tedy nejen běžné uživatele, ale i administrátory nebo externí uživatele a dodavatele.

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 přístupů a identit za užití principů *Least Privilege* a *Need to Know*.
- Pravidla a postupy pro řízení přístupových práv a oprávnění za užití principů *Least Privilege* a *Need to Know*.
- Životní cyklus řízení přístupů a identit a stanovení osob odpovědných za jednotlivé fáze.
- Životní cyklus řízení přístupových práv a oprávnění a stanovení osob odpovědných za jednotlivé fáze.
- Pravidla a postupy pro vytváření, změnu, manipulaci a obnovu autentizačních údajů, včetně postupů pro bezodkladnou změnu hesel při důvodném podezření na jejich kompromitaci.
- Pravidla a postupy pro řízení privilegovaných a administrátorských oprávnění.
- Pravidla a postupy pro řízení přístupů a identit pro mimořádné situace.
- Pravidla, postupy a evidence pro účty sloužící zejména pro případ obnovy po KBI.

- Pravidla a postupy pro pravidelné přezkoumání přístupových práv a oprávnění včetně rozdělení do jednotlivých skupin a rolí.
- Pravidla, postupy a požadavky na řízení přístupů, přístupových práv a oprávnění technických aktiv ve správě a mimo správu povinné osoby.
- Pravidla pro užívání autentizačních mechanismů a politik hesel.
- Pravidla a postupy pro omezení oprávnění k přístupu k průmyslovým, řídicím a obdobným specifickým technickým aktivům.

4.13 Politika zvládání KBU a KBI

K čemu slouží:

Politika slouží pro nastavení všech pravidel a postupů, které se týkají zvládání KBU a KBI. Politika nastavuje požadavky na detekci KBU, jejich vyhodnocování, identifikaci a zvládání KBI. Mimo jiné by měla stanovovat pravidla a postupy pro hlášení KBI na NÚKIB.

Co by měla pokrývat:

- Definování KBU a KBI.
- Pravidla a postupy pro nepřetržitou detekci, zaznamenávání a vyhodnocování KBU, včetně definování odpovědnosti za jednotlivé činnosti.
- Pravidla a postupy pro identifikaci a zvládání KBI.
- Pravidla a postupy pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu KBI.
- Pravidla a postupy testování nastavených politik a postupů pro zvládání KBI.
- Pravidla a postupy pro hlášení KBI.
- Pravidla a postupy pro vyhodnocení, řešení a určení příčiny KBI a pro pravidelné aktualizace pravidel pro vyhodnocení KBU.
- Pravidla a postupy pro hlášení KBI na NÚKIB.
- Pravidla a postupy pro evidenci KBI.
- Pravidla a postupy pro vyhodnocení účinnosti řešení KBI.

4.14 Politika řízení kontinuity činností

K čemu slouží:

Politika slouží k jasnému organizačnímu zajištění kontinuity a dostupnosti regulované služby a stanovení cílů řízení kontinuity činností. Na politiku navazují Metodika pro provedení analýzy dopadů (5.16), Plány kontinuity činností (5.18) a Plány obnovy (5.19).

Co by měla pokrývat:

- Práva a povinnosti odpovědných osob.
- Cíle řízení kontinuity činností pro jednotlivé služby.
    - Minimální úroveň poskytovaných služeb.
    - Doba obnovení chodu.

    - Bod obnovení dat.
- Priority obnovy jednotlivých primárních aktiv.
- Způsoby nouzové komunikace a hlášení.
- Komunikační matice s klíčovými osobami pro jednotlivé služby.
- Eskalační postupy pro krizové situace.
- Katalog scénářů krizových situací.
- Způsob a perioda testování jednotlivých plánů kontinuity činností a plánů obnovy.

4.15 Politika provádění auditu kybernetické bezpečnosti

K čemu slouží:

Politika slouží k nastavení pravidel pro provádění auditu kybernetické bezpečnosti tak, aby byl účinný a přínosný. Na politiku navazuje Plán provádění auditu kybernetické bezpečnosti (5.20).

Co by měla pokrývat:

- Pravidla a postupy pro provádění auditu kybernetické bezpečnosti.
- Pravidla a postupy pro plánování auditu kybernetické bezpečnosti.
- Odpovědnosti za provádění auditu kybernetické bezpečnosti.

4.16 Politika fyzické bezpečnosti

K čemu slouží:

Politika slouží k nastavení pravidel pro zajištění fyzické bezpečnosti za účelem ochrany aktiv regulované služby. Dokument by měl primárně definovat fyzické bezpečnostní perimetry pro různé úrovně zabezpečení v rámci objektů a dále pak stanovit způsoby ochrany jednotlivých perimetrů a aktiv, která se v nich nachází.

Co by měla pokrývat:

- Stanovení fyzických bezpečnostních perimetrů regulované služby a jejich úrovně fyzické ochrany.
- Pravidla a postupy pro ochranu jednotlivých úrovní fyzických bezpečnostních perimetrů regulované služby.
- Pravidla a postupy pro kontrolu a evidenci vstupu osob za účelem ochrany aktiv regulované služby.
- Pravidla a postupy pro ochranu objektů a umístěných aktiv regulované služby.
- Pravidla a postupy pro detekci narušení fyzické bezpečnosti regulované služby.
- Pravidla a postupy pro omezení fyzického přístupu k průmyslovým, řídicím a obdobným specifickým technickým aktivům regulované služby.

4.17 Politika bezpečnosti komunikačních sítí

K čemu slouží:

Politika slouží k definici pravidel a postupů pro zajištění bezpečnosti komunikační sítě poskytovatele regulované služby. Politika obsahuje mimo jiné popis nastavení pravidel na omezení a řízení komunikace v rámci komunikační sítě a jejího perimetru a nastavení pravidel pro vzdálený přístup k této síti a k jejím technickým aktivům.

Co by měla pokrývat:

- Pravidla a postupy pro zajištění segmentace sítě a oddělení jednotlivých prostředí.
- Pravidla, práva a oprávnění pro jednotlivé segmenty a prostředí s ohledem na povolení pouze nezbytné komunikace.
- Určení práv a povinností za účelem bezpečného provozu komunikační sítě.
- Pravidla a postupy pro řízení komunikace v komunikační síti.
- Pravidla a postupy pro řízení vzdáleného přístupu ke komunikační síti, a to včetně vzdáleného přístupu dodavatelů nebo jiných osob.
- Pravidla a postupy pro vzdálenou správu technických aktiv, a to včetně vzdálené správy technických aktiv dodavatelem nebo jinými osobami.
- Stanovení časového omezení vzdáleného přístupu ke komunikační síti, vzdálené správy technických aktiv a pravidel pro opětovné ověření identit.
- Pravidla a postupy pro omezení vzdálených přístupů a vzdálené správy průmyslových, řídicích a obdobných specifických technických aktiv.
- Pravidla a postupy pro užívání nástroje zajišťujícího ochranu integrity komunikační sítě.

4.18 Politika nasazení, používání a údržby nástroje pro detekci KBU a nástroje pro sběr a vyhodnocování KBU

K čemu slouží:

Politika slouží k definici pravidel a postupů pro kompletní správu nástrojů pro detekci KBU a nepřetržitou automatickou ochranu před škodlivým kódem. Řeší vše od jejich nasazení, přes nastavení pravidel, až po pravidla aktualizace a optimalizace. Politika dále slouží k nastavení pravidel a postupů pro řízení používání vyměnitelných zařízení a nosičů, automatického spouštění obsahu a ostatních zdrojů možného zanesení škodlivého kódu na technická aktiva.

Co by měla pokrývat:

- Pravidla a postupy pro nasazení, nastavení, užívání a bezodkladnou aktualizaci nástroje pro detekci KBU.
- Pravidla a postupy pro nasazení, nastavení, užívání a bezodkladnou aktualizaci nepřetržité a automatické ochrany před škodlivým kódem.
- Pravidla a postupy pro řízení a sledování používání vyměnitelných zařízení a datových nosičů.
- Pravidla a postupy pro řízení automatického spouštění obsahu a oprávnění ke spouštění kódu.
- Pravidla a postupy pro nasazení, nastavení, užívání a aktualizaci nástroje pro sběr a vyhodnocování KBU.

- Pravidla a postupy pro vyhodnocování, reagování a včasného varování určených bezpečnostních rolí na detekované KBU, včetně eskalačních postupů a kontaktů na relevantní osoby.
- Pravidla a postupy pro optimalizaci nastavení a aktualizaci pravidel pro detekci a vyhodnocování u nástroje pro sběr a vyhodnocení KBU.

4.19 Politika pro zaznamenávání událostí

K čemu slouží:

Politika slouží k nastavení pravidel a postupů pro provozování nástroje na zaznamenávání bezpečnostních a relevantních provozních událostí a pro určení konkrétních technických aktiv a jejich napojení na tento nástroj. Politika dále určuje pravidla a postupy pro nastavení samotných záznamů generovaných tímto nástrojem a dále pravidla a postupy pro synchronizaci jednotného času technických aktiv, bez kterého by zaznamenané události nešly prakticky využít.

Co by měla pokrývat:

- Pravidla a postupy pro nasazení, nastavení, užívání a aktualizaci nástroje pro zaznamenávání kybernetických bezpečnostních a relevantních provozních událostí.
- Definování rozsahu technických aktiv a určení osoby odpovědné za aktuálnost tohoto rozsahu.
- Pravidla a postupy pro napojení technických aktiv na nástroj sloužící pro sběr záznamů o událostech.
- Pravidla a postupy pro synchronizaci jednotného času technických aktiv.
- Pravidla a postupy pro jednoznačnou identifikaci technických aktiv za účelem jednoznačného určení původce zaznamenané události.
- Pravidla a postupy pro zaznamenávání činnosti administrátorů, dodavatelů a jiných privilegovaných účtů.
- Pravidla a postupy pro bezpečné zaznamenávání, uchovávání a retenci bezpečnostních a relevantních provozních událostí.

4.20 Politika aplikační bezpečnosti

K čemu slouží:

Politika slouží ke stanovení pravidel a postupů pro zajištění trvalé ochrany aplikací, informací, transakcí a přenášených identifikátorů. Toho se dá dosáhnout mimo jiné řízením jejich zranitelností, např. formou účinných aktualizací a vedením evidence výrobcem nepodporovaných, a tím pádem i zranitelných aktiv. Politika dále slouží ke stanovení pravidel a postupů pro provádění skenování zranitelností a penetračního testování, která pomáhají odhalovat další zranitelnosti.

Co by měla pokrývat:

- Pravidla a postupy pro zajištění trvalé ochrany aplikací, informací, transakcí a přenášených identifikátorů, zejména formou tzv. *Hardeningu*.
- Pravidla a postupy pro řízení, testování, nasazení a aplikování aktualizací vydaných pro technická aktiva, včetně postupů a procesů pro případné neúspěšné nasazení a obnovení původního stavu (*Rollback*).
- Pravidla a postupy pro řízení zranitelností v rámci jejich životního cyklu.
- Pravidla a postupy pro nasazování bezpečnostních aktualizací a záplat.
- Pravidla a postupy pro evidenci výrobcem, dodavatelem nebo jinou osobou nepodporovaných technických aktiv a technických aktiv, na které není možné aplikovat poslední schválenou bezpečnostní aktualizaci.
- Pravidla a postupy pro provádění pravidelného skenování zranitelností, práci s nálezy a testování zavedených bezpečnostních opatření (*Retest*).
- Pravidla a postupy pro provádění penetračního testování, práci s nálezy a testování zavedených bezpečnostních opatření (*Retest*).
- Pravidla a postupy pro evidování penetračního testování, termínu provedení a konkrétní fyzické osoby provádějící toto penetrační testování.

4.21 Politika kryptografických algoritmů

K čemu slouží:

Politika slouží k nastavení pravidel a postupů pro užívání aktuálně odolných kryptografických prostředků a zajištění zabezpečené komunikace pomocí nich. Měla by vycházet z doporučení vydanými NÚKIB pro používání prostředků.

Co by měla pokrývat:

- Pravidla a postupy pro používání a pravidelnou aktualizaci aktuálně odolných kryptografických algoritmů s ohledem na bezpečnostní standardy, doporučení a metodiky vydané NÚKIB.
- Pravidla a postupy pro zabezpečení hlasové, audiovizuální, textové (vč. e-mailové) komunikace a nouzové komunikace v rámci organizace.
- Pravidla a postupy pro využívání kryptografických klíčů a certifikátů.
- Zohlednění vlivu kvantové kryptografie.

4.22 Politika zajišťování dostupnosti regulované služby

K čemu slouží:

Politika slouží k nastavení pravidel a postupů pro zajištění dostupnosti regulované služby, jako jsou pravidla pro redundanci aktiv. Politika se dále musí věnovat nastavení pravidel a postupů pro kompletní technické zajištění záloh technických aktiv nezbytných pro zajištění regulované služby včetně manipulace s nimi a jejich oddělení v rámci komunikační sítě.

Co by měla pokrývat:

- Pravidla a postupy pro zajišťování dostupnosti regulované služby včetně redundance nezbytných aktiv.
- Pravidla a postupy pro vytváření pravidelných záloh konfigurací a nastavení technických aktiv, informací a dat nezbytných zejména pro účely obnovy regulované služby.
- Pravidla a postupy pro testování, bezpečné (šifrované) uchovávání, retenci a obnovu záloh.
- Pravidla a postupy pro řízení přístupu k zálohám a manipulaci se zálohami.
- Pravidla a postupy pro řízení bezpečné správy konfigurací technických aktiv.
- Pravidla a postupy pro bezpečné řízení zálohovacího prostředí odděleného od jiných prostředí.

4.23 Politika zabezpečení průmyslových, řídicích a obdobných technických aktiv

K čemu slouží:

Politika slouží k nastavení pravidel a postupů v rámci zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv (nejčastěji OT zařízení, SCADA řešení, relevantní servisní nástroje apod.). Požadavky na některá specifická technická aktiva se mohou lišit od požadavků kladených na ostatní technická aktiva v rámci ISMS.

Co by měla pokrývat:

- Pravidla fyzického přístupu.
- Pravidla a postupy řízení přístupových oprávnění.
- Pravidla segmentace.
- Pravidla a postupy pro omezení vzdáleného přístupu a vzdálené správy.
- Pravidla pro omezení komunikace mimo komunikační síť.
- Pravidla a postupy řízení zranitelností.
- Pravidla a postupy řízení kontinuity.

5 Obsah bezpečnostní dokumentace

5.1 Zpráva z přezkoumání ISMS

K čemu slouží:

Tato zpráva slouží jako komplexní a přehledné manažerské shrnutí o aktuálním stavu kybernetické bezpečnosti v organizaci. Měla by se tedy dotýkat všech relevantních témat, ale zároveň by neměla zacházet do zbytečných technických podrobností.

Co by měla pokrývat:

- Vyhodnocení bezpečnostních opatření z předchozího přezkoumání ISMS.
- Identifikace změn a okolností, které mohou mít vliv na ISMS.
- Zpětná vazba o účinnosti ISMS.

    - Neshody a nápravná opatření.
    - Výsledky monitorování a měření.
    - Výsledky auditu.
    - Naplnění cílů ISMS.
- Posouzení výsledků hodnocení rizik a stavu naplňování plánu zvládání rizik.
- Posouzení dopadů KBI na regulované služby a kybernetickou bezpečnost.
- Posouzení významných změn, které mohou mít negativní dopad na ISMS.
- Identifikace možností pro zlepšování.
- Doporučení potřebných rozhodnutí, stanovení bezpečnostních opatření a osob zajišťujících výkon jednotlivých činností.

5.2 Záznam z jednání výboru pro řízení kybernetické bezpečnosti

K čemu slouží:

Záznam slouží k tomu, aby bylo jednání výboru pro řízení kybernetické bezpečnosti formálně dokumentováno.

Co by měl pokrývat:

- Přítomné osoby.
- Probíraná témata.
- Přijaté závěry.

5.3 Metodika pro určování a hodnocení aktiv

K čemu slouží:

Tento dokument slouží k určení metodického postupu, na základě kterého bude prováděno určování a hodnocení aktiv. Přímo tedy souvisí se stanovením rozsahu řízení kybernetické bezpečnosti a měl by zajistit, že proces určování a hodnocení aktiv bude možné periodicky opakovat a bude přezkoumatelný.

Co by měla pokrývat:

- Pravidla a postupy pro určení 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 hodnocení primárních aktiv.
    - Určení stupnice pro hodnocení primárních aktiv z pohledu důvěrnosti, integrity a dostupnosti.
    - Zohlednění oblastí hodnocení primárních aktiv dle přílohy č. 1 vyhlášky č. 409/2025 Sb.
- Pravidla a postupy pro určení a evidenci vazeb mezi aktivy.
- Pravidla a postupy pro určení podpůrných aktiv.
- Pravidla a postupy pro evidenci podpůrných aktiv.

- Pravidla a postupy pro určení a evidenci garantů podpůrných aktiv.
- Pravidla a postupy pro hodnocení podpůrných aktiv.
    - Zohlednění vazeb mezi primárními a podpůrnými aktivy.
    - Určení stupnice pro hodnocení podpůrných aktiv.

5.4 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 primárních aktiv.
    - Určení a popis primárních aktiv souvisejících s regulovanou službou.
    - Určení a popis primárních aktiv nesouvisejících s regulovanou službou.
    - Určení garantů primárních aktiv.
    - Hodnocení primárních aktiv souvisejících s regulovanou službou z hlediska důvěrnosti, integrity a dostupnosti.
- Přehled podpůrných aktiv.
    - Určení a popis podpůrných aktiv.
    - Určení garantů podpůrných aktiv.
    - Hodnocení podpůrných aktiv z hlediska důvěrnosti, integrity a dostupnosti.
- Určení vazeb mezi primárními a podpůrnými aktivy.

5.5 Metodika pro určování a hodnocení rizik

K čemu slouží:

Dokument slouží k určení metodického postupu, na základě kterého bude prováděno určování a hodnocení rizik. Přímo tedy souvisí se stanovením rozsahu řízení kybernetické bezpečnosti a měl by zajistit, že proces řízení rizik bude možné periodicky opakovat a bude přezkoumatelný.

Co by měla pokrývat:

- Pravidla a postupy pro určování rizik.
- Pravidla a postupy pro vytvoření katalogu hrozeb.
- Pravidla a postupy pro vytvoření katalogu zranitelností.
- Stanovení vzorce pro výpočet rizik.
- Pravidla a postupy pro hodnocení rizik.
    - Určení stupnice pro hodnocení úrovní hrozby.
    - Určení stupnice pro hodnocení úrovní zranitelnosti.
    - Určení stupnice pro hodnocení úrovní rizik.
    - Pravidla a postupy pro zohlednění významných změn.
    - Pravidla a postupy pro zohlednění změn stanoveného rozsahu.

  - Pravidla a postupy pro provedení protiopatření dle § 20 zákona.
  - Pravidla a postupy pro zohlednění KBI.
  - Pravidla a postupy pro zohlednění výsledků auditů a kontrol v oblasti kybernetické bezpečnosti.
  - Pravidla a postupy pro zohlednění výsledků penetračního testování a skenování zranitelností.
- Stanovení intervalu pro provádění hodnocení rizik.
- Stanovení kritérií pro akceptovatelnost rizik.
- Pravidla a postupy pro zvládání rizik.
- Stanovení přípustných metod pro zvládání rizik (akceptace rizika, redukce a eliminace rizika, vyhnutí se riziku, přenesení nebo sdílení rizika).
- Pravidla a postupy pro výběr bezpečnostních opatření.
- Pravidla a postupy pro snižování rizik prostřednictvím zavádění bezpečnostních opatření.
- Pravidla a postupy pro schvalování akceptovatelných rizik.
- Pravidla a postupy pro práci s plánem zvládání rizik.
- Pravidla a postupy pro práci s prohlášením o aplikovatelnosti.
- Pravidla a postupy pro zpracování zprávy o hodnocení rizik.
- Pravidla a postupy pro komunikaci rizik relevantním osobám.

5.6 Hodnocení rizik

K čemu slouží:

Dokument slouží k mapování rizik prostřednictvím provedené analýzy rizik nad aktivy evidovanými v rámci stanoveného rozsahu řízení kybernetické bezpečnosti a k jejich zvládání.

Co by měla pokrývat:

- Hodnocení vhodných kombinací aktiv, hrozeb a zranitelností.
- Zohlednění zavedených bezpečnostních opatření.
- Stanovení úrovně rizik a určení způsobu zvládání rizik.
- Návrh bezpečnostních opatření a jejich realizace.

5.7 Zpráva o hodnocení rizik

K čemu slouží:

Zpráva slouží jako manažerský výstup z procesu hodnocení rizik a má za cíl poskytnout přehledný a vypovídající výstup o výsledku hodnocení rizik.

Co by měla pokrývat:

- Shrnutí procesu a výsledků hodnocení rizik.
- Shrnutí procesu zvládání rizik a navrhovaných bezpečnostních opatření.

5.8 Prohlášení o aplikovatelnosti

K čemu slouží:

Dokument slouží jako přehled o nasazených a nenasazených bezpečnostních opatřeních požadovaných vyhláškou č. 409/2025 Sb. Běžně tedy rozvádí požadavky § 3 až 27 vyhlášky č. 409/2025 Sb. a u nich uvádí stav plnění bezpečnostních opatření. U všech požadavků musí být popsáno, jak byly aplikovány, nebo odůvodněno, proč aplikovány nebyly.

Co by mělo pokrývat:

- Přehled bezpečnostních opatření požadovaných vyhláškou č. 409/2025 Sb., která nebyla aplikována včetně odůvodnění a přehledu přijatých náhradních bezpečnostních opatření.
- Přehled aplikovaných bezpečnostních opatření, včetně způsobu jejich realizace.

5.9 Plán zvládání rizik

K čemu slouží:

Dokument slouží k plánování konkrétních řešení sloužících k mitigaci identifikovaných rizik. Plán musí obsahovat všechny relevantní informace, jako je jejich popis, termín zavedení nebo samotnou provazbu na jednotlivá rizika.

Co by měl pokrývat:

- Cíle a přínosy vybraných bezpečnostních opatření pro zvládání jednotlivých rizik včetně vazby na konkrétní rizika.
- Potřebné zdroje pro jednotlivá bezpečnostní opatření pro zvládání rizik.
- Osoby zajišťující prosazování jednotlivých bezpečnostních opatření pro zvládání rizik.
- Termíny zavedení jednotlivých bezpečnostních opatření pro zvládání rizik.
- Způsob realizace bezpečnostních opatření.

5.10 Plán rozvoje bezpečnostního povědomí

K čemu slouží:

Plán by měl obsahovat údaje o tom kdo, kdy a jaká školení má absolvovat v rámci rozvoje bezpečnostního povědomí.

Co by měl pokrývat:

- Pravidla a postupy rozvoje bezpečnostního povědomí a způsoby jeho hodnocení.
    - Způsoby a formy poučení a školení uživatelů.
    - Způsoby a formy poučení a školení administrátorů.
    - Způsoby a formy poučení a školení osob zastávajících bezpečnostní role.
    - Způsoby a formy poučení a školení vrcholného vedení.
    - Způsoby a formy poučení dodavatelů.
- Vstupní školení kybernetické bezpečnosti.
- Obsah a termíny poučení a školení.

- Stanovení lhůt pro pravidelné opakování školení.

5.11 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 školení a 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 osob zastávajících bezpečnostní role.

5.12 Evidence změn

K čemu slouží:

Dokument slouží k udržení přehledu v rámci řízení změn, k určování významných změn a k mapování jejich průběhu.

Co by měla pokrývat:

- Evidenci změn, které mají nebo mohou mít vliv na kybernetickou bezpečnost.
- Určení významných změn.
- Evidenci životního cyklu významných změn.

5.13 Záznam přidělených a odebraných přístupových práv a oprávnění

K čemu slouží:

Dokument slouží k udržení aktuálního přehledu o přístupových právech a oprávněních k aktivům regulované služby, a s tím souvisejícímu zamezení výskytu nežádoucích přístupových práv a oprávnění tam, kde nemají být.

Co by měl pokrývat:

- Seznam jednotlivých identit a jejich přidělených přístupových práv a oprávnění.

5.14 Záznam KBI

K čemu slouží:

Záznamy slouží k evidenci všech KBI vč. postupů řešení pro případ nutnosti jejich dalšího řešení.

Co by měl pokrývat:

- Vedení záznamů např. pomocí tabulkového procesoru nebo ticketovacího nástroje.
- Popis jednotlivých KBI.
- Způsob jejich zvládnutí.

5.15 Závěrečná zpráva o vyřešení KBI s významným dopadem

K čemu slouží:

Tato zpráva slouží ke shrnutí a vyhodnocení vyřešeného KBI s významným dopadem včetně přijatých bezpečnostních opatření.

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.

5.16 Metodika pro provedení analýzy dopadů

K čemu slouží:

Metodika slouží k nastavení pravidel a postupů pro provádění analýzy dopadů.

Co by měla pokrývat:

- Způsoby hodnocení dopadů KBI na kontinuitu činností a posuzování souvisejících rizik.
- Způsoby identifikace kritických procesů a jejich garantů.
- Způsoby stanovení priorit pro obnovu.

5.17 Analýza dopadů

K čemu slouží:

Dokument slouží k mapování dopadů KBI na regulovanou službu a k určení priorit její obnovy.

Co by měla pokrývat:

- Posouzení možných dopadů KBI na kontinuitu činností a poskytování regulované služby.
- Určení priorit obnovy.

5.18 Plán kontinuity činností

K čemu slouží:

Plán slouží k zajištění konkrétních postupů, procesů a povinností, které zajistí, aby v případě KBI byla zachována dostupnost regulované služby. Jejich funkčnost by měla být pravidelně testována.

Co by měl pokrývat:

- Podmínky aktivace plánu.
- Specifikace osob, které se mají plánem řídit a jejich povinnosti.
- Dočasná řešení a postupy pro zajištění kontinuity služby v případě realizace krizového scénáře.
- Postupy pro spuštění a ukončení chodu technických aktiv, pro restart nebo obnovení chodu technických aktiv po selhání a pro ošetření chybových stavů nebo mimořádných jevů.

5.19 Plán obnovy

K čemu slouží:

Plán obnovy slouží jako průvodce pro obnovení poskytování regulované služby. Jeho funkčnost by měla být pravidelně testována.

Co by měl pokrývat:

- Detailní postupy pro obnovení regulované služby včetně pořadí činností, odpovědných osob, potřebného času a zdrojů.
- Umístění a popis záloh.
- Způsob ověření úspěšného obnovení ze zálohy.

5.20 Plán provádění auditu kybernetické bezpečnosti

K čemu slouží:

Dokument slouží k rozplánování auditovaných oblastí regulované služby tak, aby ve stanovené periodě proběhl audit kybernetické bezpečnosti v celém rozsahu řízení kybernetické bezpečnosti a celém rozsahu vyhlášky č. 409/2025 Sb.

Co by měl pokrývat:

- Krátkodobý a střednědobý plán auditů kybernetické bezpečnosti prováděných po dvou letech nebo po systematických celcích rozložených do pěti let.

5.21 Zpráva z auditu kybernetické bezpečnosti

K čemu slouží:

Poskytuje ucelený přehled o aktuálním stavu ISMS v organizaci.

Co by měla pokrývat:

- Cíle auditu kybernetické bezpečnosti.
- Předmět auditu kybernetické bezpečnosti.
- Kritéria auditu kybernetické bezpečnosti.
- Složení skupiny auditorů a osob, které se auditu kybernetické bezpečnosti zúčastnily.
- Datum a místo, kde byly prováděny činnosti při auditu kybernetické bezpečnosti.
- Zjištění z auditu kybernetické bezpečnosti.
- Závěry auditu kybernetické bezpečnosti.
- Nápravná opatření pro zajištění souladu s kritérii auditu kybernetické bezpečnosti.

5.22 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 vč. 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

5.23 Evidence technických aktiv, účtů a autentizačních mechanismů, které nesplňují požadavek na vícefaktorovou autentizaci

K čemu slouží:

Evidence slouží k vedení seznamu všech technických aktiv, účtů a autentizačních mechanismů, které nesplňují požadavek na vícefaktorovou autentizaci.

Co by měla pokrývat:

- Popis těchto technických aktiv, účtů a autentizačních mechanismů.
- Odůvodnění nezavedení vícefaktorové autentizace.
- Způsob nakládání s evidencí.

5.24 Evidence technických aktiv, která již nejsou podporována, a na která není možné aplikovat poslední schválenou bezpečnostní aktualizaci

K čemu slouží:

Slouží k evidování všech technických aktiv, která již nejsou podporována výrobcem. Musí tedy obsahovat jejich kompletní seznam a u každého uvedeného aktiva všechny potřebné informace, zvláště pak zavedená opatření, která zamezují zneužití jejich neošetřených zranitelností.

Co by měla pokrývat:

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

5.25 Zpráva z testování záloh

K čemu slouží:

Tyto testy slouží primárně k ověření funkčnosti záloh a jejich integrity a schopnosti organizace využít je pro řádnou a efektivní obnovu.

Co by měla pokrývat:

- Výsledky testů integrity, dostupnosti a použitelnosti vytvářených záloh.

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