LIST JAMU

Ročník 2024

částka zpřístupněna 13. listopadu 2024

OBSAH:

JAMU

Janáčkova akademie
múzických umění

SMĚRNICE

JANÁČKOVY AKADEMIE MÚZICKÝCH UMĚNÍ

ze dne 12. listopadu 2024

o systému řízení bezpečnosti informací

Kvestor vydává na základě čl. 79 vnitřního předpisu č. 12/2022 LJ, Statut Janáčkovy akademie múzických umění, tuto směrnici Janáčkovy akademie múzických umění:

ČÁST PRVNÍ

OBECNÁ USTANOVENÍ

Čl. 1

Předmět úpravy

(1) Účelem systému řízení bezpečnosti informací (dále jen „SŘBI“) je dosáhnout řízení bezpečnosti informací tak, aby bylo v souladu platnou legislativou v oblasti kybernetické bezpečnosti a současně zohledňoval strategický záměr Janáčkovy akademie múzických umění (dále jen „JAMU“), její organizační strukturu, procesy řízení, charakter aktiv a další specifika JAMU.

(2) Směrnice upravuje povinnosti vedení JAMU, strategické cíle SŘBI, pravidla pro určení rozsahu a hranic SŘBI a další pravidla a postupy související s řízením bezpečnosti informací. Zároveň vytváří organizační strukturu pro účely SŘBI.

Čl. 2

Povinnosti vedení

(1) Vedení JAMU[1)] je povinno zavedením, vzděláváním se, provozováním, prosazováním, monitorováním, přezkoumáváním, udržováním a neustálým zlepšování SŘBI. Dále je povinno vytvořit podmínky pro získávání k tomu nezbytných lidských, technických a finančních zdrojů, aktivně se podílí na řízení rizik a bere na vědomí výsledky analýzy rizik (dále jen „Strategické řízení“).

(2) Zástupcem vedení JAMU pro účely plnění povinností dle této Směrnice je Kvestor.

(3) Vedení součástí JAMU (dále jen „Vedení součástí“) se podílí v rozsahu své působnosti na plnění povinností Vedení JAMU, pakliže je daná součást zahrnuta v rozsahu SŘBI podle této Směrnicí.

Čl. 3

Cíle

(1) Vedení JAMU stanoví cíle SŘBI. V rámci toho zohlední potřeby a očekávání zainteresovaných stran. Za tímto účelem Vedení JAMU zajistí především

a) vytvoření organizační struktury a dlouhodobé zajištění personálních kapacit pro řešení SŘBI,

---

1) Čl. 69 vnitřního předpisu č. 12/2022 LJ, Statut Janáčkovy akademie múzických umění.

b) zajištění kybernetické bezpečnosti aktiv v rozsahu SŘBI,

c) nastavení potřebné úrovně a procesů průběžného rozvoje bezpečnostního povědomí všech zainteresovaných stran,

d) nastavení a průběžnou aktualizaci procesů a technologií nezbytných pro efektivní zvládání kybernetických bezpečnostních incidentů (dále jen „KBI“).

(2) Vedení JAMU stanoví krátkodobé cíle na období 1 roku a dlouhodobé cíle na období 5 let.

(3) Po uplynutí doby, pro kterou byl cíl stanoven, vedení JAMU provede vyhodnocení úrovně splnění cíle a zhodnotí dosažené výsledky a případné odchylky od stanovených cílů.

Čl. 4

Principy

Základními principy zavedení a provozování

a) princip jednotného řízení bezpečnosti informací zohledňující legislativní rámec kybernetické bezpečnosti,

b) princip jednotného řízení aktiv a rizik,

c) princip neustálého zlepšování vhodnosti, přiměřenosti a účinnosti SŘBI.

Čl. 5

Předpoklady

Mezi nutné předpoklady zavedení SŘBI patří zejména

a) obsazení bezpečnostních rolí a určení jejich práv a povinností,

b) zajištění efektivní spolupráce s odborníky i akademickou sférou v oblasti SŘBI,

c) integrace SŘBI do

1. řízení bezpečnosti a krizových a havarijních plánů JAMU,

2. řízení JAMU a plnění strategických cílů JAMU,

d) zajištění souladu s požadavky plynoucími ze zákona o kybernetické bezpečnosti, příslušnými prováděcími předpisy a normativními akty JAMU,

e) úplná a aktualizovaná dokumentace SŘBI odpovídající platné legislativě.

Čl. 6

Rozsah a hranice SŘBI

(1) Rozsah SŘBI je vymezen minimálně jako soubor aktiv potřebných k provozování regulovaných služeb v požadované kvalitě. Seznam regulovaných služeb v návaznosti na legislativní požadavky schvaluje Vedení JAMU. Rozsah SŘBI má aspekty

a) procesní, jimiž se rozumí komplexní pokrytí oblasti regulovaných služeb ve smyslu veškerých procesů spojených s realizací a nezbytných k provozování regulovaných služeb v požadované kvalitě,

b) fyzické, jimiž se rozumí všechna místa (objekty a prostory, datové sály, serverové skříně apod.), kde jsou dislokována fyzická zařízení tvořící aktiva, či jsou využívána k provozování aktiv v požadované kvalitě,

c) organizační a personální, jimiž se rozumí bezpečnostní role v rozsahu svých práv a povinností, zaměstnanci JAMU, dodavatelé a další relevantní osoby nezbytné k provozování regulovaných služeb v požadované kvalitě,

d) technologické a organizační, jimiž se rozumí veškeré informační a komunikační technologie JAMU a veškeré informační a komunikační technologie a služby poskytované dodavateli nezbytné k provozování regulovaných služeb v požadované kvalitě.

(2) Rozsah SŘBI bude stanoven dokumentem Strategický plán SŘBI. Rozsah bude aktualizován a revidován tak, aby zohledňoval aktuální potřeby a strategie JAMU alespoň 1x za rok. Změnu rozsahu SŘBI schvaluje Vedení JAMU.

Čl. 7

Pravidla a postupy pro řízení dokumentace

(1) JAMU stanoví pravidla pro efektivní řízení bezpečnostní dokumentace SŘBI, a to zejména s ohledem na

a) zajištění dostupnosti, důvěrnosti a integrity dokumentace SŘBI,

b) sledování změn a verzí dokumentace SŘBI,

c) udržování aktuální verze dokumentace SŘBI,

d) úplnost dokumentace SŘBI.

(2) Bezpečnostní dokumentace SŘBI musí být dostupná všem zainteresovaným stranám.

(3) Osoby podílející se na realizaci bezpečnostní dokumentace SŘBI mají povinnost zachovávat mlčenlivost o skutečnostech, o nichž se dozvěděli při výkonu svých povinností.

Čl. 8

Strategický plán SŘBI

(1) Manažer kybernetické bezpečnosti (dále jen „Manažer KB“) zajistí aktualizaci Strategického plánu SŘBI.

(2) Součástí tohoto dokumentu jsou alespoň

a) cíle SŘBI,

b) rozsah SŘBI JAMU,

c) zpráva o přezkoumání SŘBI,

d) nápravná opatření,

e) výstupy Vedení součásti.

Čl. 9

Politiky SŘBI

(1) Politiky SŘBI představují souhrn povinností osob podílejících se na SŘBI pro jednotlivé oblasti SŘBI

a) řízení aktiv,

b) řízení rizik,

c) řízení dodavatelů,

d) řízení lidských zdrojů,

e) řízení provozu a komunikací,

f) řízení přístupu,

g) bezpečného chování,

h) technické zabezpečení aktiv,

i) mobilních zařízení,

j) fyzické bezpečnosti,

k) řízení změn,

l) monitorování a řízení bezpečnostních aktivit,

m) řízení kontinuity činností.

(2) Politiky SŘBI budou reflektovat aktuální zákonné požadavky.

(3) Manažer KB navrhuje Vedení JAMU Politiky SŘBI, zároveň zajistí jejich revizi, a to vždy minimálně 1x ročně.

ČÁST DRUHÁ

OSOBY ŘÍDÍCÍ KYBERNETICKOU BEZPEČNOST

Hlava I

Obecné ustanovení

Čl. 10

Na řízení SŘBI se podílí osoby zastávajících bezpečnostní role, Výbor kybernetické bezpečnosti (dále jen „Výbor KB“), kvestor a Vedení součásti ve stanoveném rozsahu podle této Směrnice.

Hlava II

Bezpečnostní role

Čl. 11

(1) Bezpečnostní role představují organizačně strukturovaný systém osob, které se podílejí na realizaci SŘBI v rozsahu práv a povinností, které jim adresují bezpečnostní politiky JAMU nebo nadřazené bezpečnostní role v rozsahu jejich oprávnění.

(2) Bezpečnostními rolemi na JAMU jsou

a) Manažer KB,

b) pověřenec kybernetické bezpečnosti (dále jen „Pověřenec KB“),

c) gestor kybernetické bezpečnosti (dále jen „Gestor KB“),

d) garant primárního aktiva,

e) garant podpůrného aktiva.

(3) V případě, že osoba zastávající bezpečnostní roli poruší své povinnosti stanovené SŘBI, bude porušení individuálně posouzeno a v závislosti na jeho závažnosti, opakování a dalších okolností budou vyvozeny opatření k nápravě.

Hlava III

Výbor KB

Čl. 12

Působnost Výboru KB

Výbor KB

a) odpovídá za celkové řízení a rozvoj kybernetické bezpečnosti v rámci povinné osoby,

b) schvaluje návrh a rozsah SŘBI,

c) definuje strategické cíle a směřování rozvoje v oblasti kybernetické bezpečnosti,

d) definuje role a odpovědnosti v rámci SŘBI,

e) definuje požadavky na vnitřní komunikaci a kontrolu SŘBI, a kontrolu aktuálního stavu kybernetické bezpečnosti a dohledu nad dodržováním stanovených cílů,

f) prosazuje a podporuje SŘBI,

g) seznamuje se s relevantními výstupy souvisejícími s řízením kybernetické bezpečnosti,

h) účastní se školení kybernetické bezpečnosti,

i) projednává významné KBI,

j) projednává nápravná opatření.

Čl. 13

Výbor KB a jeho složení

(1) Kvestor ustavuje Výbor KB jako svůj vrcholný poradní sbor pro kybernetickou bezpečnost.

(2) Výbor KB se skládá z

a) kvestora jako zástupce Vedení JAMU a Rektorátu, který je jeho předsedou,

b) tajemnice Hudební fakulty JAMU,

c) tajemnice Divadelní fakulty JAMU,

d) ředitelů ostatních součástí JAMU,

e) vedoucího Oddělení výpočetních a informačních služeb Rektorátu JAMU,

f) administrátora informačních a komunikačních technologií,

g) manažera KB.

(3) Člena Výboru KB podle odstavce 3 písm. f) povolá k výkonu jeho povinností kvestor.

Čl. 14

Předseda a místopředseda

(1) Předseda řídí zasedání a činnost Výboru KB a vystupuje jako reprezentant Výboru KB navenek. Předseda může pověřit řízením zasedání jiného člena Výboru KB.

(2) Výbor KB si může ze svých členů zvolit místopředsedu, který předsedu zastupuje v době jeho nepřítomnosti či zaneprázdněnosti.

Čl. 15

Práva a povinnosti členů

(1) Členové Výboru KB mají právo vznášet dotazy, náměty, připomínky k projednávaným zprávám a návrhům a uplatňovat svá stanoviska k řešení projednávaných problémů.

(2) Členové Výboru KB jsou povinni podílet se aktivně na činnosti Výboru KB, účastnit se jeho zasedání osobně a plnit úkoly, kterými je Výbor KB pověřil, nebrání-li jim v účasti vážné důvody.

Čl. 16

Informování členů Výboru KB

Pozvánku na zasedání, program zasedání a podklady, zápis o zasedání a jiné dokumenty a informace týkající se činnosti Výboru KB budou členům Výboru KB zpřístupňovány prostřednictvím sdíleného uložiště s řízeným přístupem.

Čl. 17

Svolání zasedání

(1) Zasedání svolává předseda Výboru KB podle potřeby, nejméně však jednou za kalendářní čtvrtletí.

(2) O termínu zasedání Výboru KB vyrozumí předseda členy zpravidla nejméně 2 týdny přede dnem zasedání s uvedením dne, místa, času a navrhovaného programu zasedání spolu s potřebnými podklady. V odůvodněných případech mohou být podklady zpřístupněny až při zahájení zasedání. Člen může navrhnout zařazení bodu do programu zasedání Výboru KB.

(3) Vyžaduje-li to projednávaná věc, může předseda přizvat na zasedání i další osoby.

Čl. 18

Průběh zasedání

(1) Předsedající na úvod zasedání oznámí, zda zasedání bylo řádně svoláno, ověří usnášeníschopnost Výboru KB, určí zapisovatele a předloží ke schválení změny či doplnění programu zasedání.

(2) Jednotlivé body programu postupně uvede předsedající nebo jím pověřená osoba jako zpravodaj. Poté je k danému bodu zahájena rozprava.

(3) Předsedající přečte na závěr zasedání znění přijatých rozhodnutí a jiné podstatné body zápisu. Zasedání končí oznámením předsedajícího o ukončení zasedání.

Čl. 19

Rozhodování mimo zasedání

(1) Je-li věc rozhodována mimo zasedání (per rollam), rozešle předseda členům Výboru KB podklady k takto projednávané věci a zjišťovací otázky, na něž je třeba k vyřízení věci odpovědět.

(2) Členové Výboru KB ve stanovené přiměřené lhůtě na položené otázky odpoví a mohou se k projednávané věci i jinak vyjádřit.

Čl. 20

Usnášeníschopnost

Výbor KB je usnášeníschopný, je-li na zasedání účastna nebo vyjádří-li se při jednání per rollam většina všech členů.

Čl. 21

Většina k přijetí rozhodnutí

K přijetí rozhodnutí Výboru KB je třeba souhlasu většiny účastných nebo při jednání per rollam vyjádřivších se členů.

Čl. 22

Zápis

(1) O každém zasedání nebo rozhodování per rollam se pořídí zápis, který se rozešle členům Výboru KB a na vědomí rektorovi, případně těm, kterých se týká.

(2) V zápisu o zasedání se vždy uvede, kdo zasedání svolal, kdy a kde k zasedání došlo, kdo byl zasedání účasten a kdo mu předsedal, jaký byl schválený program zasedání, výsledek jednotlivých hlasování, znění případně přijatých rozhodnutí a datum jeho sepsání.

(3) V zápisu o jednání per rollam se uvedou položené otázky, hlasy jednotlivých členů, výsledek jednotlivých hlasování a datum jeho sepsání.

Hlava IV

Kvestor

Čl. 23

Kvestor představuje osobu odpovědnou za realizaci práv a povinností Strategického řízení. Za tímto účelem Kvestor

a) zajišťuje dostupnost zdrojů potřebných pro SŘBI,

b) svěřuje Manažerovi KB řízení konkrétního KBI,

c) zajišťuje integraci SŘBI do procesů JAMU,

d) zajišťuje informování zaměstnanců o významu SŘBI a významu dosažení shody s jeho požadavky se všemi dotčenými stranami,

e) zajistí podporu k dosažení cílů SŘBI,

f) prosazuje neustálé zlepšování SŘBI,

g) poskytuje Manažerovi KB nezbytnou součinnost za účelem plnění jeho povinností,

h) schvaluje po projednání Výborem KB dokumentaci předloženou Manažerem KB podle této Směrnice,

i) v případě, že je Manažer KB anebo osoby provádějící audit kybernetické bezpečnosti (dále jen „Audit KB“) realizován prostřednictvím dodavatele, řídí tohoto dodavatele pro účely SŘBI,

j) seznamuje se SŘBI v rozsahu nezbytném pro plnění svých povinností,

k) prokazatelně se účastní jemu určenému školení.

Hlava V

Manažer KB

Čl. 24

Povolání, postavení a požadavky

(1) Manažera KB jmenuje kvestor. Manažer KB je organizačně podřízen kvestorovi.

(2) Výkonem bezpečnostní role Manažera KB může být pověřena osoba, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s řízením kybernetické bezpečnosti v rozsahu legislativních požadavků stanovených pro tuto bezpečnostní roli.

Čl. 25

Působnost Manažera KB

(1) Manažer KB

a) spolupracuje s Pověřencem KB, kvestorem a Výborem KB při implementaci požadavků regulace KB do prostředí JAMU, včetně metodické podpory jejich povinností stanovených touto Směrnicí,

b) navrhuje rozsah SŘBI JAMU, navrhuje a metodicky řídí SŘBI JAMU, včetně bezpečnostních předpisů a dokumentace, reflektujících požadavky relevantních právních předpisů, potřeby JAMU a ustanovení této Směrnice,

c) řídí jednotlivé bezpečnostní role přímo anebo prostřednictvím pokynů udělených Pověřenci KB,

d) navrhuje bezpečnostní požadavky a bezpečnostní opatření,

e) poskytuje pravidelný reporting minimálně v rozsahu 1x měsíčně pro kvestora. V rámci reportingu bude zohledněn: vývoj SŘBI, významné změny KBI, to vše za reportované období. V tomto ohledu uděluje pokyny Pověřenci KB za účelem sběru informací z prostředí JAMU,

f) pravidelně komunikuje s kvestorem. V tomto ohledu uděluje pokyny Pověřenci KB za účelem sběru informací z prostředí JAMU,

g) poskytuje metodickou podporu Pověřenci KB a relevantním bezpečnostním rolím podle bezpečnostních předpisů JAMU, při zohlednění legislativních požadavků kybernetické bezpečnosti v rámci vytváření, hodnocení, výběru, řízení a ukončení dodavatelských vztahů majících dopad na SŘBI JAMU. Zároveň poskytuje metodickou podporu při návrhu obsahu dokumentů vytvářejících či ukončujících dodavatelský vztah, či dokumentů takovýto vztah vybírající, hodnotící a řídící,

h) zajišťuje komunikaci dle aktuální potřeby v souvislosti s opatřeními vydanými Národním úřadem pro kybernetickou a informační bezpečnost („NÚKIB“) a při hlášení kybernetické bezpečnostních incidentů,

i) řídit KBI za podpory poskytnuté Pověřencem KB případně dalšími relevantními bezpečnostními rolemi podle bezpečnostních předpisů JAMU. Spolupracuje při tom s orgány činnými v trestním řízení a NÚKIB,

j) vytvoří Plán rozvoje bezpečnostního povědomí,

k) v souladu s plánem rozvoje bezpečnostního povědomí zajistí pravidelné školení a ověřování bezpečnostního povědomí bezpečnostních rolí, Vedení JAMU a Výboru KB, ostatních zaměstnanců v souladu s jejich pracovní náplní,

l) hodnotí účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených se zlepšováním bezpečnostního povědomí,

(2) Manažer KB předkládá Výboru KB k projednání

a) zprávu o hodnocení aktiv a rizik,

b) plán zvládání rizik,

c) návrh SŘBI, včetně jeho průběžné aktualizace,

d) prohlášení o aplikovatelnosti,

(3) U dokumentů uvedených v odstavci 2 tohoto článku Manažer KB

a) poskytuje metodickou podporu a pokyny při zpracování uvedených dokumentů Pověřenci KB a relevantním bezpečnostním rolím podle bezpečnostních předpisů JAMU,

b) uvedené dokumenty kompletuje na základě podkladů získaných Pověřencem KB a relevantními bezpečnostními rolemi podle bezpečnostních předpisů JAMU.

(4) Manažer KB se v rozsahu SŘBI

a) podílí na schvalování závazných požadavků pro výběr, unifikaci a systemizaci technických a programových prostředků informačních technologií JAMU,

b) podílí na organizaci kontrol etap dílčích plnění,

c) je informován o zkušebním a ověřovacím provozu a zátěžových testech,

d) podílí na přípravě testovacích dat a organizaci bezpečnostních testování,

e) podílí po věcné stránce na formulaci požadavků veřejných zakázek včetně zakázek malého rozsahu.

(5) Manažer KB je také oprávněn úkolovat osoby neuvedené mezi bezpečnostními rolemi v rozsahu jejich organizačního zařazení a právního vztahu mezi těmito osobami a JAMU, za účelem realizace SŘBI, a to prostřednictvím vedoucího pracoviště. Vedoucí pracoviště zajistí, aby byla předmětná osoba seznámena s rozsahem požadovaných opatření a zajistí jejich dodržování. Předmětná osoba má povinnost dodržovat stanovené požadavky.

Hlava VI

Pověřenec KB

Čl. 26

Obecné vymezení role

Pověřenec KB je organizační role zajišťující realizaci SŘBI pod dohledem Manažera KB. Za tímto účelem především zajišťuje zprostředkování informací z prostředí JAMU, poskytuje součinnost Manažerovi KB a zajišťuje sběr informací spojených s prostředím JAMU pro účely SŘBI, a to podle pokynů Manažera KB.

Čl. 27

Činnost pověřence

(1) Pověřenec KB zejména

a) monitoruje činnosti spojené se SŘBI, zejména

1. realizaci bezpečnostních opatření,

2. dodržování bezpečnostní politik,

3. plnění plánu zvládání rizik,

b) ve spolupráci s Manažerem KB identifikuje jednotlivá aktiva a jejich vzájemné vazby a garanty,

c) pověřuje ostatní bezpečnostní role povinnostmi SŘBI,

d) zpracovává bezpečnostní dokumentaci v souladu s metodickou podporou Manažera KB,

e) zajišťuje řešení kybernetické bezpečnostní události/incidentu v případě, že

1. kvestorem nebyl povolán Manažer KB,

2. v rozsahu pověření Manažera KB,

3. pokud tak vyplývá z bezpečnostních předpisů JAMU,

f) zajišťuje hlášení kontaktních údajů a jejich změn u NÚKIB,

g) dle metodických pokynů Manažera KB realizuje proces řízení rizik,

h) kontroluje dodržování povinností, provádí konkrétní školení podle pokynů Manažera KB,

i) vede o školení přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly,

j) v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role zajistí předání odpovědností,

k) v souladu s plánem rozvoje bezpečnostního povědomí zajistí poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení,

l) prokazatelně se účastní jemu určenému školení,

m) dohlíží na vkládání dokumentů podle této směrnice do zabezpečeného uložiště a nastavuje přístupová oprávnění dalších osob.

(2) Jednotlivé činnosti stanovené Pověřenci KB mohou vykonávat ostatní bezpečnostní role JAMU v souladu s bezpečnostními předpisy JAMU.

Hlava VII

Gestor KB

Článek 28

Povolání a postavení

(1) Gestor KB odpovídá v rozsahu své působnosti za řízení aktiv a řízení rizik v souladu s Politikami SŘBI (dále jen „Taktické řízení“).

(2) Roli Gestora KB vykonává Kvestor. Gestor KB je metodicky podřízený Manažerovi KB.

(3) Je-li potřeba, může Kvestor vyzvat Manažera KB, aby na návrh Vedení součásti určil dedikovaného Gestora KB pro tuto součást JAMU; Gestor KB pro součást spolupracuje také na strategickém řízení.

Hlava VIII

Garanti aktiv

Čl. 29

Garant primárního aktiva

(1) Garant primárního aktiva je odpovědný správu primárního aktiva spočívající v zajištění rozvoje, použití a bezpečnosti primárního aktiva.

(2) Garant primárního aktiva je organizačně podřízený příslušnému Gestorovi KB a metodicky Manažerovi KB.

(3) Garant primárního aktiva je určen a plní povinnosti v souladu s Politikami SŘBI, na základě kterých bude ve stanoveném rozsahu pro typ jím spravovaného aktiva, a podle

potřeb daného aktiva odpovídat za povinnosti stanovené ostatními Politikami SŘBI garantovi aktiv.

Čl. 30

Garant podpůrného aktiva

(1) Garant podpůrného aktiva je odpovědný za správu podpůrného aktiva spočívající v zajištění rozvoje, použití a bezpečnosti podpůrného aktiva.

(2) Garant podpůrného aktiva je organizačně podřízený příslušnému Gestorovi KB a metodicky Manažerovi KB.

(3) Garant podpůrného aktiva je určen a plní povinnosti v souladu s politikami SŘBI na základě kterých bude ve stanoveném rozsahu pro typ jím spravovaného aktiva a podle potřeb daného aktiva odpovídat za povinnosti stanovené ostatními Politikami SŘBI garantovi aktiv.

ČÁST TŘETÍ

OVĚŘOVÁNÍ A NÁPRAVA

Čl. 31

Audit KB

(1) Vedení JAMU v rámci Auditu KB v rozsahu SŘBI

a) určí osobu provádějící Audit KB,

b) stanoví program Auditů KB, včetně četnosti Auditu KB,

c) výsledky Auditu KB zohlední v rámci stanovení cílů SŘBI ve smyslu Článku 3 této Směrnice.

(2) Audit KB musí být prováděn osobou vyhovující podmínkám stanoveným právním rámcem kybernetické bezpečnosti, která nezávisle hodnotí správnost a účinnost zavedených bezpečnostních opatření.

Čl. 32

Důvod a periodicita Auditu KB

(1) Audit KB je prováděn: při významných změnách v rámci jejich rozsahu a v pravidelných intervalech alespoň po 3 letech.

(2) Není-li v odůvodněných případech možné provést Audit KB v určených intervalech v celém rozsahu SŘBI, je možné Audit KB provádět průběžně po systematických celcích. V takovém případě je nutno Audit KB v celém rozsahu provést nejpozději do 5 let od posledního celkového Auditu KB.

Čl. 33

Výstup Auditu KB

Výstup Auditů KB musí obsahovat alespoň posouzení souladu bezpečnostních opatření s nejlepší praxí, právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky a určení případných nápravných opatření pro zajištění souladu.

Čl. 34

Pravidla a principy pro přezkum SŘBI

(1) Pravidelné přezkoumání SŘBI probíhá každý rok a obsahuje hodnocení současného stavu, trendů, cílů SŘBI a příležitostí pro další rozvoj, posouzení funkčnosti a efektivnosti zavedených postupů a procesů, eventuálně nutnost případných změn tak, aby byla zajištěna vhodnost, přiměřenost a efektivnost SŘBI.

(2) Přezkum SŘBI

a) provádí vedení JAMU za pomoci ostatních bezpečnostních rolí,

b) výsledkem je Zpráva o přezkoumání SŘBI, kterou schvaluje Vedení JAMU,

c) pro přezkum SŘBI slouží definované vstupy.

Čl. 35

Vstupy pro přezkoumání SŘBI

Vstupy pro přezkoumání SŘBI zahrnují:

a) vyhodnocení nápravných opatření z předchozího přezkoumání SŘBI,

b) změny a okolnosti, které mohou mít vliv na SŘBI,

c) zpětnou vazbu o výkonnosti SŘBI (neshody a nápravná opatření, výsledky monitorování a měření, výsledky kontrol a auditů, plnění cílů SŘBI),

d) výsledky hodnocení rizik a stav plnění plánu zvládání rizik,

e) Hodnocení úrovně zavedených bezpečnostních opatření,

f) Výstupy ze skenování zranitelností a penetračního testování,

g) Přehled kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů za uplynulé období,

h) Vyhodnocení plnění cílů stanovených v Strategickém plánu SŘBI,

i) Vyhodnocení plánu vzdělávání v oblasti kybernetické bezpečnosti.

Čl. 36

Výstupy přezkoumání SŘBI

Výstupem přezkoumání SŘBI je Zpráva o přezkoumání SŘBI, která musí zahrnovat zejména pokyny směřující

a) ke zvyšování účinnosti SŘBI,

b) k aktualizaci hodnocení rizik a plánu zvládání rizik,

c) k nezbytným změnám postupů/metodik/politik bezpečnosti informací, v reakci na vnitřní nebo vnější události, které by mohly mít vliv na SŘBI,

d) k potřebě zdrojů,

e) ke zlepšování postupů měření účinnosti přijatých opatření.

Čl. 37

Pravidla a postupy pro nápravná opatření a zlepšování SŘBI

(1) Veškerá nápravná opatření vychází z pokynů uvedených ve Zprávě z přezkoumání SŘBI. Tato nápravná opatření jsou projednána Výborem KB. Jednotlivým nápravným opatřením jsou stanoveny osoby odpovědné za zavedení nápravných opatření a dodržení termínu zavedení nápravného opatření.

(2) Nápravná opatření jsou projednávána Výborem KB, dokud nejsou implementována. Výbor KB uchovává dokumentované informace jako důkaz o povaze neshod a všech následně přijatých opatřeních a o výsledcích nápravných opatření.

(3) Pokud vyjde najevo nesplnění požadavku SŘBI, považuje se taková skutečnost za neshodu. V takovém případě musí Výbor KB

a) reagovat na neshodu a případně přijmout opatření k její kontrole a nápravě a vypořádat se s následky,

b) vyhodnotit potřebu opatření k odstranění příčin neshody, aby se neopakovala nebo nevyskytovala jinde,

c) přezkoumat účinnost přijatých nápravných opatření,

d) v případě potřeby provést změny v SŘBI.

(4) Dlouhodobý přístup k neustálému zlepšování musí zahrnovat měření účinnosti SŘBI, přijatých procesů a opatření. Kombinace účinných procesů monitorování, měření a nápravných opatření spolu s formálním procesem přezkoumání a silnou strukturou interního auditu umožní Vedení JAMU prokázat svůj přístup k neustálému zlepšování.

ČÁST ČTVRTÁ

ÚČINNOST

Čl. 38

Tato směrnice nabývá účinnosti 18. listopadu 2024.

Ing. Dana Horníčková, v. r.

kvestorka

Obsah