Jihočeská univerzita v Českých Budějovicích

Označení dokumentu:	**ISMS-001**
Název dokumentu:	**Politika systému řízení bezpečnosti informací**
Typ dokumentu:	Interní dokument – **TLP:GREEN**
Rozsah:	Politika má nastínit strategické cíle SŘBI, rozsah a hranice SŘBI a další pravidla a postupy související s řízením SŘBI.
Prvek legislativy:	Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti § 5
Datum vydání:	07. 07. 2026
Datum účinnosti:	**07. 07. 2026**
Platnost do:	odvolání
Počet stran + příloh:	3 + 0
Verze:	1.1
Význam a benefity:	Význam politiky je poskytnout nasměrování a podporu pro řízení bezpečnosti informací v souladu s příslušnými platnými zákony a předpisy.
Uložení:	Sekce kyberbezpečnosti na Wiki JU
Ruší dokumenty:	-
Zpracovatel:	Manažer KB JU
Přezkoumal:	Výbor pro kybernetickou bezpečnost JU
Schválil:	Výbor pro kybernetickou bezpečnost JU

Informační vyhlášení

SŘBI se skládá z politik, postupů, směrnic a souvisejících zdrojů a činností, které JU společně spravuje za účelem ochrany svých informačních aktiv.

a) Cíle, principy a potřeby řízení bezpečnosti informací

Zavedení SŘBI patří mezi stěžejní organizační bezpečnostní opatření pro zajištění bezpečnosti informací VIS.

Při zavádění SŘBI se berou v úvahu následující základní principy:

- povědomí o potřebě řízení bezpečnosti informací;
- přidělení odpovědnosti za bezpečnost informací;
- začlenění závazku vedení k řízení bezpečnosti informací;
- posouzení rizik, které určuje vhodné kontrolní mechanismy k dosažení přijatelné úrovně rizik;
- začlenění bezpečnosti jako základního prvku informačních sítí a systémů;
- aktivní prevence a odhalování incidentů v oblasti bezpečnosti informací;
- zajištění komplexního přístupu k řízení bezpečnosti informací;
- průběžné přehodnocování bezpečnosti informací a provádění případných úprav.

Stanovené cíle musí být měřitelné.

b) Rozsah a hranice systému řízení bezpečnosti informací

Smyslem stanovení rozsahu je určit organizační části a aktiva, jichž se SŘBI týká, tedy fyzický perimetr, organizační celky, zainteresované osoby a technologie.

Dle vyhlášky o kybernetické bezpečnosti je rozsah SŘBI nutno stanovit dokumentovanou formou a s ohledem na požadavky dotčených stran a organizační bezpečnost. Dokumentované stanovení rozsahu SŘBI je nezbytné pro následnou přezkoumatelnost, případnou potřebu jeho rozšíření, či pro zajištění jeho jednotného výkladu v organizaci.

Stanovení rozsahu a hranic SŘBI je detailněji popsáno v příloze č. 1 této politiky.

c) Politiky systému řízení bezpečnosti informací

Základní politika (tzn. hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací) vyhlášená vedením je dostupná také všem zainteresovaným stranám na Wiki JU v sekci Kyberbezpečnost. Žádný aspekt a činnost systému bezpečnosti informací nesmí být v rozporu s touto základní politikou.

JU stanovuje dílčí bezpečnostní politiky v oblasti systému řízení bezpečnosti informací minimálně v rozsahu podle přílohy č. 5 k vyhlášce č. 82/2018 Sb.

d) Pravidla a postupy pro řízení dokumentace

Bezpečnostní dokumentace je kontrolována manažerem KB JU. Verzování a dostupnost dokumentace všem zaměstnancům je zajištěna prostřednictvím Wiki JU v sekci kyberbezpečnost.

Stanovené strukturované číslování bezpečnostní dokumentace na JU je:

- ISMS-X-YYY – Název dokumentu
    - X[1] = Typ dokumentu; S-Směrnice, O-Opatření, D-Důvěryhodné
    - YYY = číslo dokumentu

JU zajistí, aby:

- bylo pravidelně kontrolováno aktuální vydání dokumentu,
- aby byly sledovány a kontrolovány změny a verze,
- aby byla dokumentace úplná a
- aby byla vedena historie dokumentace.

e) Pravidla a postupy pro řízení zdrojů a provozu systému řízení bezpečnosti informací

JU přidělí přiměřené zdroje (finanční, lidské, technické) potřebné k zavedení a udržování principů vedoucích ke zvyšování kybernetické bezpečnosti.

f) Pravidla a postupy pro provádění auditů kybernetické bezpečnosti

JU v rámci auditu kybernetické bezpečnosti:

- provádí a dokumentuje audit dodržování bezpečnostní politiky, včetně přezkoumání technické shody, a výsledky auditu zohlední v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik a
- posuzuje soulad bezpečnostních opatření s nejlepší praxí, právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k VISu a určí případná nápravná opatření pro zajištění souladu.

Audit je prováděn:

- při významných změnách, v rámci jejich rozsahu,
- v pravidelných intervalech alespoň po 3 letech dle §16 písm. b) vyhlášky o kybernetické bezpečnosti a

Není-li v odůvodněných případech možné provést audit v určených intervalech v celém rozsahu, je možné audit provádět průběžně po systematických celcích. V takovém případě je nutno audit v celém rozsahu provést nejpozději do 5 let.

Audit kybernetické bezpečnosti musí být prováděn osobou vyhovující podmínkám stanoveným v § 7 odst. 4 vyhlášky o kybernetické bezpečnosti (včetně možnosti využití externího dodavatele auditních služeb), která nezávisle hodnotí správnost a účinnost zavedených bezpečnostních opatření.

Výbor pro řízení kybernetické bezpečnosti JU předkládá výsledky auditu kybernetické bezpečnosti správci daného informačního a komunikačního systému a vedení JU.

g) Pravidla a postupy pro přezkoumání systému řízení bezpečnosti informací

JU musí přezkoumat:

[1] Politiky ISMS znak nevyužívají.

- bezpečnostní politiky a bezpečnostní dokumentaci,
- soulad technických a organizačních opatření s bezpečnostními politikami.

Výsledky přezkoumání zdokumentovat, uchovávat a při neshodě zaznamenat případná navržená nápravná opatření.

h) Pravidla a postupy pro nápravná opatření a zlepšování systému řízení bezpečnosti informací

Pokud se vyskytne neshoda, musí JU:

- reagovat na neshodu a případně přijmout opatření k její kontrole a nápravě a vypořádat se s následky;
- vyhodnotit potřebu opatření k odstranění příčin neshody, aby se neopakovala nebo nevyskytovala jinde;
- přezkoumat účinnost přijatých nápravných opatření a
- v případě potřeby provést změny v systému řízení bezpečnosti informací.

JU uchová zdokumentované informace jako důkaz o povaze neshod a všech následně přijatých opatřeních a o výsledcích nápravných opatření.

JU je povinna neustále zlepšovat vhodnost, přiměřenost a účinnost SŘBI. JU přijme vhodný a přiměřený proces neustálého zlepšování, např. PDCA, v kontextu SŘBI.

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 JU začít prokazovat svůj přístup k neustálému zlepšování.

S implementací účinných měření může pomoci norma ISO/IEC 27004.

Historie revizí

Historie revizí je uvedena u souboru této politiky na Wiki JU.