Jihočeská univerzita v Českých Budějovicích

Označení dokumentu:	**ISMS-010**
Název dokumentu:	**Politika bezpečného předávání a výměny informací**
Typ dokumentu:	Interní dokument – **TLP:GREEN**
Rozsah:	Tato politika se vztahuje na všechny zaměstnance, organizační oddělení a uživatele zdrojů a prostředků IT.
Prvek legislativy:	Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti § 10, 26
Datum vydání:	07. 07. 2026
Datum účinnosti:	**07. 07. 2026**
Platnost do:	odvolání
Počet stran + příloh:	2 + 0
Verze:	1.1
Význam a benefity:	Při předávání informací v rámci VVŠ, mezi VVŠ, nebo jinými stranami, je nutné zabránit jejich ztrátě, úpravě nebo zneužití.
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

JU musí zavést formální zásady, postupy a kontrolní mechanismy v rámci SŘBI, které budou sloužit na ochranu výměny určených informací prostřednictvím jakýchkoli komunikačních prostředků, včetně dopisů, e-mailů, hlasové a video komunikace. Tyto postupy stanoví zaměstnancům, jak a s kým komunikovat a co se od nich očekává při použití některého z komunikačních prostředků. Bezpečné předávání informací musí být součástí školení všech zaměstnanců.

a) Pravidla a postupy pro ochranu předávaných informací

Pravidla a postupy musí zahrnovat:

- postupy určené k ochraně vyměňovaných informací (včetně osobních údajů) před zachycením, kopírováním, úpravou, nesprávným směrováním a zničením
  - tyto postupy musí zahrnovat technologické opatření, jakými jsou, ku příkladu, digitální podpis, šifrování a jiné kryptografické techniky na ochranu důvěrnosti, integrity a autenticity
    - způsob ochrany informací musí odpovídat stupni klasifikaci informací
- odkazy na politiku ochrany před škodlivým kódem, politiku přijatelného používání a formální pokyny pro výměnu, uchovávání a likvidaci informací
- bezpečné postupy výměny informací prostřednictvím bezdrátové komunikace
- připomenutí zaměstnancům, že mají sdělovat důvěrné informace jen ze zabezpečených míst
  - což nejsou veřejná místa, otevřené kanceláře, kanceláře s tenkými stěnami apod.

Školení zaměstnanců musí zahrnovat kapitolu o nepovoleném použití komunikačních kanálů VVŠ: k čemukoliv nezákonnému, co může narušit chod VVŠ, nebo co by mohlo ohrozit důvěryhodnost nebo pověst VVŠ.

b) Způsoby ochrany elektronické výměny informací

JU musí mít formální dohody o způsobech ochrany elektronické výměny informací. Otázky, které by měly být řešeny v dohodách, závisí na citlivosti informací. Dohody musí obsahovat všechny příslušné zásady a postupy, které JU uplatňuje při výměně informací, a musí zahrnovat:

- stanovené odpovědnosti a závazky v případě incidentů v oblasti bezpečnosti informací,
- dohodnutý systém označování, aby bylo zajištěno, že požadovaná odpovídající ochrana je okamžitě zřejmá a zajištěná,
- případné zvláštní kontroly (např. kryptografické), které mohou být nezbytné pro zvláště citlivé informace.

c) Pravidla pro využívání kryptografické ochrany

Informace zpracovávána v rámci VIS musí být chráněna proti zneužití vhodnými kryptografickými metodami, které zajistí pouze autentizovaný a autorizovaný přístup k těmto informacím.

Pravidla pro využívání kryptografické ochrany musí zahrnovat situace, ve kterých se nachází nebo nalézají data organizace a určení vhodné úrovně kryptografické ochrany pro dané situace.

VIS musí být připraven využívat aktuálně bezpečné kryptografické algoritmy dle doporučení NÚKIB. V případě použití jiného, než doporučeného algoritmu musí být toto použití řádně odůvodněno.

Historie revizí

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