



Jihočeská univerzita v Českých Budějovicích

<i>Označení dokumentu:</i>	ISMS-000
<i>Název dokumentu:</i>	Základní politika bezpečnosti informací
<i>Kategorie TLP:</i>	TLP: CLEAR
<i>Rozsah:</i>	Politika je určena pro všechny zaměstnance, studenty a účastníky celoživotního vzdělávání JU, dodavatele a organizace spolupracující s JU nebo jiné zainteresované strany.
<i>Prvek legislativy:</i>	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti
<i>Datum vydání:</i>	6. 12. 2024
<i>Datum účinnosti:</i>	6. 12. 2024
<i>Platnost do:</i>	odvolání
<i>Počet stran + příloh:</i>	2 + 0
<i>Verze:</i>	1.0
<i>Význam a benefity:</i>	Význam politiky je definovat hlavní zásady, cíle, bezpečnostní potřeby a práva a povinnosti ve vztahu k řízení bezpečnosti informací na Jihočeské univerzitě v Českých Budějovicích pro všechny zainteresované strany.
<i>Uložení:</i>	Veřejná část wiki stránek JU
<i>Ruší dokumenty:</i>	
<i>Zpracovatel:</i>	Jan Urbánek - Manažer KB JU
<i>Přezkoumal:</i>	Výbor pro řízení kybernetické bezpečnosti JU
<i>Schválil:</i>	Rektor JU

Informační vyhlášení

Tato politika je vydána na základě zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, a jeho prováděcích předpisů, zejména vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

Tato politika je součástí bezpečnostní politiky v oblasti systému řízení bezpečnosti informací v rámci Jihočeské univerzity v Českých Budějovicích (dále jen „JU“).

Bezpečnostní politika dále navazuje v rámci zajištění kybernetické bezpečnosti JU na opatření rektora R 511¹.

a) Hlavní zásady, cíle a bezpečnostní potřeby

JU si uvědomuje existenci reálných hrozeb v oblasti kybernetické bezpečnosti a důležitost zajištění kybernetické bezpečnosti na JU (dále jen „KB JU“) pro bezproblémové naplňování poslání a činností JU.

JU si uvědomuje svoji odpovědnost za KB JU, a proto se zavazuje, že bude v souladu se strategií JU aktivně podporovat adekvátní zajištění KB JU.

JU se zároveň bude aktivně podílet na hodnocení efektivnosti systému řízení bezpečnosti informací (dále jen „SŘBI“), zajištění KB JU a bude poskytovat odpovídající zdroje nutné k dosažení cílů KB JU.

Pro dosažení výše uvedených zásad se JU zavazuje:

- Ustanovit a zavést SŘBI společně s určením rozsahu a hranice celého systému,
- Provozovat, monitorovat, přezkoumávat, udržovat a kontinuálně zlepšovat SŘBI (tzv. PDCA cyklus),
- Zajistit vymezení cílů SŘBI a plánu jejich dosažení,
- Určit role, práva a povinnosti v oblasti SŘBI,
- Provádět interní audity SŘBI,
- Zajistit zdroje pro veškeré etapy životního cyklu SŘBI.

Pojmem **bezpečnost informací** se rozumí proces zajišťování ochrany informací na potřebné úrovni z hlediska kontinuálního zabezpečení jejich integrity, dostupnosti a důvěrnosti.

Hlavní cíle JU v oblasti KB jsou zajistit, že:

- Informační aktiva JU jsou odpovídajícím způsobem chráněna z hlediska výše uvedeného pojmu bezpečnosti informací,

¹ Opatření rektora R 511, k zajišťování kybernetické bezpečnosti na JU

- Bezpečnostní rizika informačních aktiv spojená s chodem JU jsou efektivně řízena,
- Jsou nastaveny a kontrolovány procesy k zajištění KB,
- Bezpečnostní opatření jsou v souladu s platnou legislativou kybernetické bezpečnosti České republiky nebo vycházejí z mezinárodně uznávaných standardů a doporučení.

Jednotlivé bezpečnostní cíle se naplňují pomocí zavádění adekvátních personálních, organizačních, procesních či technických opatření, určených v rámci procesu řízení rizik a v souladu s legislativními požadavky a relevantními standardy či normami.

b) Práva a povinnosti ve vztahu k řízení bezpečnosti informací

Veškerý popis práv a povinností jednotlivých rolí je ve vztahu k řízení bezpečnosti informací upraven v opatření rektora R 511¹.

c) Rozsah a hranice systému SŘBI JU

SŘBI JU se vztahuje na všechny pracoviště a součásti JU, všechny zaměstnance, studenty a účastníky celoživotního vzdělávání JU. Dále předmětem rozsahu SŘBI v rámci JU jsou veškeré informace, aktiva, podpůrná aktiva, procesy a jiné procedury, které se účastní na provozu významných informačních systémů JU. Do rozsahu SŘBI spadají i služby a výrobky poskytované externími dodavateli, které se podílí na provozu významných informačních systémů JU.

SŘBI JU zahrnuje všech 23 oblastí bezpečnostní politiky podle vyhlášky o kybernetické bezpečnosti.

d) Zpracování dokumentace KB A SŘBI JU

Jednotlivé politiky, směrnice, procedury a procesy, metodické příručky a další informace spojené s KB a SŘBI JU jsou výhradně interního charakteru a budou dostupné pouze zaměstnancům či studentům JU a účastníkům ČŽV. Veškeré interní dokumenty KB a SŘBI JU jsou přístupné pouze po přihlášení na webových stránkách Wiki JU - <https://wiki.jcu.cz/>.

Předmětnou výjimku tvoří tato Základní politika bezpečnosti informací, včetně všech příloh a ostatních souvisejících dokumentů, které jsou výslovně uvedeny.

Historie revizí

Verze 1.0 – Vytvoření dokumentu