



Jihočeská univerzita v Českých Budějovicích

<i>Označení dokumentu:</i>	ISMS-015
<i>Název dokumentu:</i>	Politika fyzické bezpečnosti
<i>Typ dokumentu:</i>	Interní dokument – TLP:GREEN
<i>Rozsah:</i>	Definovat nový či rozšířit stávající soubor opatření předcházející poškození, krádeži či zneužití aktiv či majetku nebo přerušení poskytování služeb informačního a komunikačního systému, vymežit fyzický perimetr.
<i>Prvek legislativy:</i>	Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti § 4, 17
<i>Datum vydání:</i>	07. 07. 2026
<i>Datum účinnosti:</i>	07. 07. 2026
<i>Platnost do:</i>	odvolání
<i>Počet stran + příloh:</i>	2 + 0
<i>Verze:</i>	1.1
<i>Význam a benefity:</i>	Stanovení základních požadavků a principů pro zajištění bezpečnosti informací z pohledu fyzické bezpečnosti.
<i>Uložení:</i>	Sekce kyberbezpečnosti na Wiki JU
<i>Ruší dokumenty:</i>	-
<i>Zpracovatel:</i>	Manažer KB JU
<i>Přezkoumal:</i>	Výbor pro kybernetickou bezpečnost JU
<i>Schválil:</i>	Výbor pro kybernetickou bezpečnost JU

Informační vyhlášení

Zajištění fyzické bezpečnosti doplňuje bezpečnost informací o fyzickou vrstvu, kde se informace nacházejí.

a) Pravidla pro ochranu objektů

Oblast, ve které jsou uchovávány a zpracovávány informace a umístěna technická aktiva informačního a komunikačního systému jsou Fyzickým bezpečnostním perimetrem, který je nutné vymezit, chránit a zabezpečit:

- před neoprávněným vstupem,
- před poškozením, neoprávněnými zásahy, a
- pro zajištění ochrany na úrovni objektů a v rámci objektů.

JU musí zajistit ochranu hlavně kritických míst perimetru (např. serverovny, kanceláře zaměstnanců, technologické místnosti, archivy, datové sklady), ale také objektů samotných.

Perimetr musí být fyzicky odolný (tj. neměly by být žádné mezery v perimetru nebo místech, kde by mohlo snadno dojít k vloupání). Střecha, stěny a podlaha perimetru musí mít pevnou konstrukci a všechny vnější dveře musí být vhodně chráněny proti neoprávněnému přístupu za pomoci kontrolních mechanismů (např. alarmy, zámky). Dveře a okna bez dozoru musí být uzamčeny a je třeba zvážit vnější ochranu u oken, zejména v 1. NP a 2. NP.

b) Pravidla pro kontrolu vstupu osob

Všechny osoby se musí při vstupu do perimetru jednoznačně autentizovat. Při zjištění incidentu (pohybu neoprávněné osoby, narušení perimetru) je stanoven a prováděn postup, kterým je informován bezpečnostní personál perimetru. Tento postup je součástí pravidelného školení zaměstnanců (recepčních).

Přístupová práva musí být pravidelně přehodnocována, aktualizována, případně revokována.

JU musí definovat pravidla pro návštěvy, např. vstup pouze s doprovodem, identifikace návštěvy při vstupu do prostoru apod.

Čas a datum příchodu a odchodu osoby musí být zaznamenány. Všechny osoby musí být v doprovodu oprávněné osoby, pokud jejich přístup nebyl předem schválen (např. vyplývá z uzavřených smluv). Osoby musí být instruovány ohledně bezpečnostních požadavků pro vstup do perimetru a ohledně pohotovostních procesů.

Kniha návštěv, či už fyzická nebo elektronická, musí být bezpečně udržována a monitorována a související logy uchovávány.

c) Pravidla pro ochranu zařízení

Technická aktiva informačního a komunikačního systému musí být zabezpečena proti přístupu neautorizovaných osob a musí být situována do takových prostor, aby nedošlo k jejich odcizení.

Zařízení v perimetru musí být alespoň částečně chráněna před potenciálními přírodními hrozbami, jakými jsou např. oheň, výbuch, voda, prach apod. Rovněž jsou zavedeny postupy pro případy selhání dodávaných služeb (výpadek klimatizace, výpadek dodávky energie). Z důvodu prevence musí být v perimetru monitorovány fyzikální veličiny prostředí, jakými jsou např. teplota a vlhkost. Zařízení musí být chráněna před výpadkem napájení a přepětím.

Musí být zavedena pravidla pro chování osob (stravování, pití, kouření atp.) v perimetru.

Každá budova musí být opatřena hromosvodem a proudovými a přepětiovými ochranami silových rozvodů dle platných norem. Rovněž jsou prováděny pravidelné revize.

Komunikační, napájecí a obslužné trasy různých vedení/rozvodů z/do perimetru musí být adekvátně chráněny a vzájemně odděleny.

d) Detekce narušení fyzické bezpečnosti

V perimetru je instalován kamerový systém se záznamem.

Monitorovací systémy a systémy detekce nepovoleného vstupu jsou pravidelně testovány.

Monitorování musí zahrnovat všechna kritická místa – všechny dveře a přístupná okna, další místnosti, vstupy, chodby, rozvodny apod.

Historie revizí

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