

Politika ochrany fyzické bezpečnosti

I. Úvodní ustanovení

- 1) Politika ochrany fyzické bezpečnosti stanovuje pravidla a postupy pro zajištění fyzické bezpečnosti aktiv a rozpracovává požadavky na kybernetickou bezpečnost dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále také „zákon o kybernetické bezpečnosti“) a 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), ve znění pozdějších předpisů (dále také „vyhláška o kybernetické bezpečnosti“) v podmínkách Univerzity Hradec Králové (dále také „UHK“).
- 2) Účelem politiky je zajistit bezpečný provoz prostředků pro zpracování informací, služeb a procesů v souladu s bezpečnostními požadavky a potřebami. Zajištěním bezpečnosti se zde rozumí předcházení poškození, krádeži nebo zneužití aktiv nebo přerušení poskytování služeb informačních systémů UHK.
- 3) Tato politika je závazná pro všechny zaměstnance UHK a také přiměřeně pro zaměstnance třetích stran, kteří mohou za předem definovaných podmínek do prostor UHK vstupovat.

II. Pravidla pro ochranu objektů

- 1) Oblast, ve které jsou uchovávány a zpracovávány informace a umístěna technická aktiva informačního a komunikačního systému jsou fyzickým bezpečnostním perimetrem, který je vymezen, chráněn a zabezpečen:
 - a) před neoprávněným vstupem,
 - b) před poškozením, neoprávněnými zásahy a
 - c) pro zajištění ochrany na úrovni objektů a v rámci objektů.
- 2) Z hlediska fyzické ochrany je stanovena a dokumentována kategorizace prostor a minimální rozsah organizačních opatření a rozsah systémů technické ochrany, ve kterých jsou umístěny prvky informačních a komunikačních technologií:
 - a) prostory kategorie „I“ – společné prostory, ve kterých jsou umístěny prvky informačních a komunikačních technologií UHK,
 - b) prostory kategorie „II“ – uzamykatelné kanceláře a místnosti, ve kterých jsou umístěny pracovní stanice,
 - c) prostory kategorie „III“ – režimové technologické místnosti, ve kterých jsou umístěny podružné rozvaděče se síťovými prvky vnitřní sítě,
 - d) prostory kategorie „IV“ – režimové serverovny a datová centra.
- 3) Kategorie konkrétních prostor určují Garanti příslušných aktiv.

- 4) Narušení fyzické bezpečnosti IS se považuje za kybernetickou bezpečnostní událost případně za kybernetický bezpečnostní incident a je zaznamenáno do nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí.

III. Pravidla pro kontrolu vstupu osob

- 1) Veškeré objekty, ve kterých se nachází technická aktiva informačních a komunikačních systémů jsou zabezpečeny proti přístupu neoprávněných osob nastavenými režimovými opatřeními.
- 2) 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.
- 3) Přístupová práva jsou pravidelně přehodnocována, aktualizována, případně revokována.

IV. Pravidla pro ochranu zařízení

- 1) Technická aktiva informačních a komunikačních systémů jsou zabezpečena proti přístupu neautorizovaných osob a jsou situována do takových prostor, aby nedošlo k jejich odcizení.
- 2) Požadavky na ochranu zařízení k zabezpečení pracovišť UHK jsou stanoveny v jednotlivých provozních řádech. Tyto provozní řády obsahují mimo jiné povolené přístupy a vlastníky privilegií ke správě zařízení.

V. Detekce narušení fyzické bezpečnosti

- 1) Narušení fyzické bezpečnosti je detekováno pracovníky fyzické ostrahy, popř. detekčním systémem napojeným na ústřednu PZTS. V případech, kdy narušení fyzické bezpečnosti detekují vlastní zaměstnanci UHK je jejich povinností o této skutečnosti informovat pracovníky fyzické ostrahy, popř. Policii ČR. Postup na hlášení bezpečnostních incidentů je formálně popsán v provozním řádu daného pracoviště.
- 2) Monitorování prostor s technickými aktivy informačních a komunikačních systémů a detekce narušení prostor je v působnosti Technicko-provozního oddělení UHK.

VI. Závěrečná ustanovení

Politika ochrany fyzické bezpečnosti vstupuje v platnost i účinnost dnem jejího podpisu.

V Hradci Králové dne 31. 5. 2024

prof. Ing. Kamil Kuča, Ph.D., v. r.
rektor