

Politika bezpečného předávání a výměny informací

I. Úvodní ustanovení

- 1) Politika bezpečného předávání a výměny informací stanovuje pravidla a způsob ochrany pro předávání informací 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 této politiky je zavést formální zásady, postupy a kontrolní mechanismy v rámci systému řízení bezpečnosti informací (dále také „SŘBI“), které budou sloužit na ochranu výměny určených informací prostřednictvím jakýchkoliv komunikačních prostředků. Tyto postupy stanoví zaměstnancům UHK, 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 UHK.

II. Pravidla a postupy pro ochranu předávaných informací

- 1) K ochraně přenosu informací prostřednictvím všech druhů komunikačních zařízení jsou stanoveny postupy a opatření na základě klasifikace informací.
- 2) Dochází-li k předávání informací s externím subjektem (např. smluvní strana), podrobnosti o bezpečném předávání informací jsou definovány dohodou o předávání informací.
- 3) Dohoda o předávání informací obsahuje zejména:
 - a) rozsah předávaných informací,
 - b) způsob zabezpečení předávaných informací, včetně ochrany důvěrnosti, integrity a dostupnosti,
 - c) účel užití předávaných informací,
 - d) technické parametry předávaných informací,
 - e) odpovědnosti a povinnosti v případě vzniku kybernetického bezpečnostního incidentu a kybernetické bezpečnostní události,
 - f) dohodu o mlčenlivosti (NDA).
- 4) Za uzavření dohody o předávání informací odpovídá Garant příslušného aktiva, jehož aktivum je se smluvní stranou sdíleno.

- 5) Pro předávání informací je zakázáno využívat veřejná internetová úložiště.
- 6) Uveřejňování informací na internetových stránkách UHK je řízeno.

III. Způsoby ochrany elektronické výměny informací

- 1) Na ochranu elektronicky předávaných informací jsou použita opatření v souladu s *Politikou řízení aktiv*.
- 2) Na ochranu nosičů elektronicky předávaných informací jsou použita opatření v souladu s *Politikou řízení aktiv*.
- 3) Informace publikované na veřejně přístupných IS (webové stránky UHK) je nutno chránit proti neoprávněné modifikaci.

IV. Pravidla pro využívání kryptografické ochrany

- 1) Kryptografická opatření jsou používána v případech nutnosti zajistit důvěrnost, integritu a dostupnost přenášených informací v souladu s klasifikací aktiv.
- 2) Používání prostředků kryptografické ochrany se řídí *Politikou bezpečného používání kryptografické ochrany*.

V. Závěrečná ustanovení

Politika bezpečného předávání a výměny informací vstupuje v platnost i účinnost dnem jejího podpisu.

V Hradci Králové dne 31. 5. 2024

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