

Politika bezpečného používání kryptografické ochrany

I. Úvodní ustanovení

- 1) Politika bezpečného používání kryptografické ochrany stanovuje pravidla a postupy bezpečného používání kryptografické ochrany 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 zajištění důvěrnosti aktiv v oblasti digitální komunikace.
- 3) Tato politika se vztahuje na všechny uživatele, veškerou komunikaci a citlivé informace, ve vztahu ke všem datům a informacím dle jejich klasifikace.

II. Úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu

- 1) Úroveň ochrany s využitím kryptografického algoritmu je dokumentována a řízena pro každý prvek informační a komunikační technologie.
- 2) Na základě analýzy rizik primárních aktiv je stanovena požadovaná úroveň ochrany s ohledem na:
 - a) kategorizaci informací primárních aktiv,
 - b) použití přenosového média,
 - c) typ a sílu kryptografického algoritmu.

III. Pravidla kryptografické ochrany informací

- 1) Pravidla pro použití kryptografické ochrany jsou dokumentována a řízena.
- 2) Na UHK jsou používány aktuálně odolné kryptografické algoritmy a kryptografické klíče.
- 3) Aktualizace kryptografických algoritmů je prováděna minimálně v souladu s doporučením Národního úřadu pro kybernetickou a informační bezpečnost (dále také „NÚKIB“). Správci mají povinnost při nastavení systémů tato doporučení dodržovat, což pravidelně dokládají v záznamu kontrol.
- 4) Pro vybrané prvky informačních a komunikačních technologií jsou používána kryptografická opatření za účelem zajištění:

- a) identifikačních a autentizačních prostředků,
 - b) autorizačních prostředků,
 - c) přenosu informací mezi prvky informačních a komunikačních technologií,
 - d) šifrování souborů,
 - e) zabezpečení elektronické pošty a přístupu k internetu.
- 5) Opatření kryptografické ochrany informací jsou implementována při přenosu po komunikačních sítích:
- a) mezi segmenty sítí UHK,
 - b) při přístupu do vnitřní sítě UHK z vnějšího prostředí,
 - c) při výměně informací mezi IS.
- 6) Opatření kryptografické ochrany informací jsou implementována při uložení souborů na mobilní zařízení nebo vyměnitelné technické nosiče dat a je použita jedna z těchto metod:
- a) šifrování na úrovni celých disků,
 - b) šifrování na úrovni virtuálních disků,
 - c) šifrování na úrovni souborů.

IV. Systém správy klíčů

- 1) Systém správy klíčů je rozdělen na oblast:
- a) centrální správa klíčů,
 - b) zaměstnanecké kryptografické klíče,
 - c) kryptografické klíče systémových účtů,
 - d) kryptografické klíče certifikačních autorit.
- 2) Systém centrální správy klíčů zajišťuje vydávání certifikátů a klíčů, jejich obnovu, zneplatnění a archivaci.

- 3) Zaměstnanecké kryptografické klíče jsou používány výhradně pro:
 - a) autentizaci ve vnitřní síti a vytváření interního elektronického podpisu,
 - b) vytváření kvalifikovaného elektronického podpisu v souladu se zvláštními právními předpisy.
- 4) Kryptografické klíče systémových účtů slouží k šifrování dat na úrovni prvků informačních a komunikačních technologií a k šifrování přenosu dat mezi prvky informačních a komunikačních technologií.
- 5) Technické parametry importu kryptografických klíčů od kvalifikovaných poskytovatelů certifikačních služeb jsou stanoveny na základě smluvního vztahu mezi UHK a kvalifikovaným poskytovatelem certifikačních služeb.
- 6) Po celou dobu existence kryptografického klíče probíhá monitoring jeho stavu a expirace.

V. Závěrečná ustanovení

Politika bezpečného používání kryptografické ochrany vstupuje v platnost i účinnost dnem jejího podpisu.

V Hradci Králové dne 31. 5. 2024

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