Politika bezpečného chování uživatelů

I. Úvodní ustanovení

1) Politika bezpečného chování uživatelů stanovuje pravidla bezpečného chování uživatelů za účelem zajištění bezpečnosti informací a snížení rizik výskytu kybernetického bezpečnostního incidentu a kybernetické bezpečnostní události na významných informačních systémech (dále také *„VIS"*) 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) V rámci působnosti bezpečnostní politiky jsou implementována pravidla pro užívání informačních a komunikačních technologií UHK, která jsou detailně rozpracována *Provozním řádu ICT UHK*[1].

3) Účelem této implementované bezpečnostní politiky je:

   a) definovat zásady bezpečného chování uživatelů,

   b) stanovit povinnosti uživatelů,

   c) definovat pravidla bezpečného provozu VIS.

4) Tato politika se vztahuje na všechny uživatele informačních a komunikačních technologií UHK, kteří využívají možnosti, prostředky, služby počítačové sítě a informační a komunikační technologie provozované VIS UHK.

II. Pravidla pro bezpečné nakládání s aktivy

1) Pravidla pro zacházení s aktivy jsou stanovena na základě zejména jejich klasifikace a jsou dokumentována pro každé aktivum dle *Klasifikace aktiv*.

2) Uchovávání, ukládání a archivace informací, dat a procesů je prováděno tak, aby byla zajištěna jejich dostatečná ochrana před neoprávněným přístupem a aby bylo znemožněno jejich jiné zneužití.

3) Každý uživatel má přístup pouze k těm aktivům, která nezbytně potřebuje k výkonu své pracovní náplně.

4) Případné výjimky z pravidel jsou realizovány na základě odůvodněné a schválené žádosti. Žádost schválí přímý nadřízený žadatele a postoupí ji Manažerovi kybernetické

[1] V době vydání této politiky je tímto předpisem rektorském výnosem č. 4/2017.

bezpečnosti (dále také *„Manažer KB"*), který ji schválí nebo zamítne a postoupí ji vedoucímu Oddělení informačních technologií (dále také *„OIT"*) k technické realizaci.

III. Bezpečné použití přístupového hesla

1) Přístup k počítačové síti předpokládá nutnost jednoznačné identifikace každého uživatele. S každým jednotlivým uživatelským účtem jsou spojena určitá přístupová práva, která rozhodujícím způsobem určují oprávnění uživatele ve vztahu k aktivům VIS.
2) Uživatel je povinen zabezpečit svůj uživatelský účet heslem a toto heslo udržovat v tajnosti a nesdělovat jiné osobě.
3) Uživatel nesmí zpřístupnit svůj uživatelský účet jiným uživatelům počítačové sítě UHK.
4) Uživatel je povinen respektovat pravidla tvorby a nakládání s přístupovými hesly, která jsou uvedeny v aktuální verzi na webových stránkách UHK.

IV. Bezpečné použití elektronické pošty a přístupu na internet

1) V rámci elektronické pošty jsou nastaveny následující pravidla:
   a) Zaměstnanci jsou povinni pravidelně kontrolovat obsah schránky elektronické pošty a schránku udržovat funkční. Důsledky plynoucí z případného nepřijetí informace (např. z důvodu přeplnění schránky) nese v plné míře adresát.
   b) Informace obsažené v elektronicky předávaných zprávách je nutno přiměřeně chránit. U informací s vysokou úrovní důvěrnosti jsou vyžadovány kryptografické prostředky pro jejich ochranu.
   c) Uživatelé mohou používat elektronickou poštu pouze k plnění pracovní činnosti. Je zakázáno zneužívat elektronickou poštu k reklamním a jiným účelům, sloužícím k získání osobního prospěchu. OIT si vyhrazuje právo systémově omezit doručování zpráv s charakteristikou nevyžádané pošty (spam) a blokovat nebezpečný obsah v elektronické poště (např. nebudou doručovány zavirované soubory).
   d) Při použití elektronické pošty je zakázáno otevírat přílohy a webové odkazy z e-mailů od neznámých zdrojů. V případě výskytu podezřelého e-mailu je uživatel povinen nahlásit tuto skutečnost Manažerovi KB nebo OIT.
   e) Veškerý provoz počítačové sítě je z bezpečnostních důvodů monitorován. Tyto údaje jsou využívány pro statistické účely a pro potřeby řešení bezpečnostních incidentů.
2) V rámci přístupu na internet jsou nastaveny následující pravidla:
   a) Přidělování přístupových práv je omezeno provozními možnostmi počítačové sítě. Schvalovat přístup k blokovaným zdrojům v rámci internetu a dalších externích počítačových sítí je v pravomoci vedoucího OIT. Seznam aktuálně povolených portů je k dispozici na oficiálních webových stránkách UHK.
   b) Technickými prostředky může být blokován přístup na nežádoucí zdroje v rámci sítě internet. V případě, že jsou blokovány zdroje nezbytné pro pracovní nebo

studijní činnost na UHK, je možnost požádat správce OIT o uvolnění konkrétních zdrojů. Je nepřípustné stahování obsahu z webových stránek s nežádoucím obsahem (erotické, vulgární, propagující nenávist, politickou, náboženskou a rasovou agitaci, dále pak nelegálně poskytovaný software a multimediální soubory chráněné autorským zákonem), a to i v případě, že stahování obsahu není blokováno síťovými prostředky.

V. Bezpečný vzdálený přístup

1) Bezpečný vzdálený přístup do vnitřních sítí UHK je dokumentovaný a řídí se těmito pravidly:
   a) je povolen pouze na základě žádosti předané vedoucímu OIT a schválené Manažerem KB,
   b) pro vzdálený přístup k aktivům VIS musí uživatelé využít schválené technologie,
   c) vytvořené spojení v rámci vzdáleného přístupu je šifrované a předchází mu autentizace uživatele,
   d) přístupy jsou jednoznačně zaznamenány spolu s identifikací uživatele,
   e) uživatelé nesmí sdílet své oprávnění vzdáleného přístupu.
2) Uživatelé prostředků umožňujících vzdálený přístup jsou povinni neprodleně provádět všechny doporučené aktualizace a úpravy prostředků umožňujících vzdálený přístup tak, aby byla minimalizována rizika jejich zneužití pro neoprávněný přístup k aktivům VIS UHK.

VI. Bezpečné chování na sociálních sítích

1) Uživatelé, kteří nemají v popisu práce využívání a správu oficiálních účtů UHK na sociálních sítích, nejsou oprávnění využívat prostředky UHK k přístupu k sociálním sítím.
2) Uživatelé, do jejichž pracovní náplně spadá využívání a správa oficiálních účtů UHK na sociálních sítích, dodržují pravidla bezpečné práce se sociálními sítěmi, zejména:
   a) dbají na ochranu přihlašovacích údajů, dostatečnou komplexnost hesla, jeho důvěrnost a pravidelnou obměnu,
   b) využívají sociální sítě pouze pro oficiální potřeby UHK a sdílejí pouze takové informace, které jsou v souladu s oficiální komunikační politikou a zájmy UHK.

VII. Bezpečnost ve vztahu k mobilním zařízením

Bezpečnost ve vztahu k mobilním zařízením se řídí *Politikou bezpečného používání mobilních zařízení*.

VIII. Závěrečná ustanovení

Politika bezpečného chování uživatelů vstupuje v platnost i účinnost dnem jejího podpisu.

V Hradci Králové dne 31. 5. 2024

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