UNIVERZITA PARDUBICE	
Opatření rektora č. 4/2022	
Věc:	Zabezpečení uživatelských účtů zaměstnanců multifaktorovou autentizací
Působnost:	všechny útvary Univerzity Pardubice
Účinnost:	8. 4. 2022
Číslo jednací:	RPO/0010/22
Vypracoval a předkládá:	Ing. Jiří Slanina, manažer kybernetické bezpečnosti
Schválila:	doc. Ing. Liběna Černohorská, Ph.D., prorektorka pro vnitřní záležitosti

Článek 1
Úvodní ustanovení

1) Rektor Univerzity Pardubice (dále jen „univerzita“) vydává toto opatření za účelem zvýšení zabezpečení informačních systémů univerzity vzhledem k následujícím důvodům:
   a) Univerzita je ve svěřené působnosti v oblasti veřejné správy orgánem veřejné moci, na který se vztahují ustanovení zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, a jeho prováděcích předpisů.
   b) Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) v rámci preventivních kroků vydal v souvislosti s kritickou hrozbou kyberšpionáže a dalších kybernetických útoků varování, v němž nabádá organizace řídící se zákonem o kybernetické bezpečnosti, k ostražitosti proti nejčastěji používaným technikám útoků a k provedení aktualizace informačních systémů a jejich komponent tak, aby nedocházelo ke zneužití známých zranitelností.
   c) V hodnocení kybernetických incidentů, které NÚKIB zveřejňuje na svých webových stránkách, je zmíněn rostoucí trend v kybernetické bezpečnosti v oblasti tzv. *phishingu*, *spear-phishingu* a sociálního inženýrství s následnou kompromitací uživatelských účtů.
   d) V rámci porady vedení univerzity dne 13. 12. 2021 v návaznosti na doporučení Výboru pro kybernetickou bezpečnost byl ze strany vedení univerzity pověřen manažer kybernetické bezpečnosti koordinací zvýšení zabezpečení informačních systémů univerzity postupným nasazením multifaktorové autentizace (dále jen „MFA“) pro bezpečné přihlašování.

Článek 2
Harmonogram nasazení MFA

1) Rektor tímto opatřením ukládá vedoucím útvarů přímo podřízených rektorovi, prorektorům, kvestorovi nebo děkanům, aby:
   a) do 14 dnů od nabytí účinnosti tohoto opatření u zaměstnanců příslušného útvaru stanovili, jaký způsob zabezpečení (alespoň jedna metoda MFA) ve smyslu čl. 3 odst. 1 tohoto opatření bude u jednotlivých zaměstnanců použit, resp. v případě, kdy není metoda MFA u konkrétního zaměstnance vyžadována (nepřiděleno NetID/nepřistupuje k informačním systémům), zvolili variantu „nebude používat MFA“, a tuto informaci prostřednictvím formuláře dostupného na https://zamestnanci.upce.cz/uredni-sdeleni v sekci Výboru pro řízení kybernetické bezpečnosti předali manažerovi kybernetické bezpečnosti;
   b) nejpozději do 30. 4. 2022 zajistili, že zaměstnanci příslušného útvaru, kteří jsou vůči univerzitě v pracovním poměru, budou mít způsob zabezpečení stanovený dle písm. a)

tohoto odstavce zaregistrovaný v portálu https://mojeheslo.upce.cz; podrobnosti způsobu registrace zvolené metody pro realizaci MFA jsou k dispozici v návodu pro MFA na https://servicedesk.upce.cz;

c) nejpozději do 30. 9. 2022 zajistili, že jim podřízení zaměstnanci, jejichž vztah vůči univerzitě vyplývá z uzavřené dohody o provedení práce nebo dohody o pracovní činnosti, budou mít způsob zabezpečení stanovený dle písm. a) tohoto odstavce zaregistrovaný v portálu https://mojeheslo.upce.cz; podrobnosti způsobu registrace zvolené metody pro realizaci MFA jsou k dispozici v návodu pro MFA na https://servicedesk.upce.cz.

2) Rektor dále ukládá vedoucí OPM nejpozději do 30. 4. 2022 ve spolupráci s manažerem kybernetické bezpečnosti navrhnout a zrealizovat změny v dokumentech a postupech souvisejících se vznikem a skončením pracovněprávních vztahů, které zahrnou nastavení metody MFA a správu poskytnutých bezpečnostních tokenů do standardních procesů univerzity.
3) Rektor dále ukládá manažerovi kybernetické bezpečnosti ve spolupráci s Centrem informačních technologií a služeb (dále jen „CITS“) na základě dat získaných dle odst. 1 tohoto článku stanovit potřeby hardwarového vybavení a harmonogram nasazování MFA na jednotlivých fakultách, celouniverzitních útvarech a rektorátních útvarech (dále jen „harmonogram“) a informovat o něm vedení univerzity. Na základě harmonogramu ukládá CITS podniknout nezbytné kroky k jeho realizaci.
4) Aktuální seznam informačních systémů chráněných MFA vč. harmonogramu a seznam použitelných hardwarových prostředků včetně dalších podrobností je dostupný na https://zamestnanci.upce.cz/uredni-sdeleni v sekci Výboru pro řízení kybernetické bezpečnosti.

Článek 3
Způsob realizace MFA

1) MFA bude na univerzitě realizována některou z těchto metod:
   a) zasíláním potvrzovacích SMS kódů,
   b) využitím ověřovací aplikace nainstalované na chytrém mobilním telefonu nebo
   c) využitím fyzického zařízení pro elektronické ověření identity uživatele (tzv. bezpečnostní token).
2) Zaměstnanci, kterým je ze strany univerzity poskytován služební mobilní tarif, si zaregistrují metodu MFA podle odst. 1 písm. a) nebo b) tohoto článku prostřednictvím https://mojeheslo.upce.cz (návod pro MFA je k dispozici na https://servicedesk.upce.cz).
3) Zaměstnancům, kterým nebyl ze strany univerzity poskytnut služební mobilní tarif, univerzita v případě jejich zájmu umožní realizovat MFA prostřednictvím soukromého telefonu podle odst. 1 písm. a) nebo b) tohoto článku nebo soukromého bezpečnostního tokenu podle odst. 1 písm. c) tohoto článku.
4) Zaměstnancům, kterým nebyl ze strany univerzity poskytnut služební telefon a kteří neprojeví zájem o využití soukromého telefonu nebo soukromého bezpečnostního tokenu, bude zaregistrována MFA služebním bezpečnostním tokenem podle odst. 1 písm. c) tohoto článku v souladu s harmonogramem.
5) Technické požadavky a technickou podporu metody MFA poskytuje Oddělení správy výpočetní techniky.
6) Standardní proces pořizování a správu bezpečnostních tokenů podle odst. 1 písm. c) tohoto článku zajišťuje CITS. Žádost o poskytnutí bezpečnostního tokenu podá příslušný vedoucí zaměstnanec prostřednictvím univerzitního systému https://servicedesk.upce.cz.

7) Náklady spojené s pořízením bezpečnostního tokenu, případně služebního telefonu se hradí z prostředků útvaru, na kterém je příslušný zaměstnanec zaměstnán.

Článek 4
Závěrečná ustanovení

1) Toto opatření nabývá platnosti a účinnosti dnem podpisu rektora.

V Pardubicích dne 8. 4. 2022

prof. Ing. Libor Čapek, Ph.D.
rektor