



PEDAGOGICKÁ
FAKULTA
Univerzita Karlova

OPATŘENÍ DĚKANA Č. 11/2026

Č. j. UKPedF/392963/2026

Zpracovala: bezpečnostní koordinátor fakulty, vedoucí SIT.

Odpovídá: děkan fakulty.

Pravidla kybernetické bezpečnosti na Pedagogické fakultě Univerzity Karlovy

ČÁST PRVNÍ ÚVODNÍ USTANOVENÍ

Čl. 1

Úvodní ustanovení

1. Toto opatření děkana vychází z Opatření rektora č. 35/2024 a Opatření rektora č. 18/2026 a stanovují se jím terminologie, pravidla, postupy a bezpečnostní opatření v oblasti bezpečného nakládání s informacemi a prostředky informačních a komunikačních technologií (ICT), které jsou závazné pro všechny zaměstnance Pedagogické fakulty Univerzity Karlovy (dále jen „fakulty“) včetně zaměstnanců vykonávajících práci na základě dohody o provedení práce nebo dohody o pracovní činnosti a také včetně externích pracovníků (dále jen „zaměstnanec“).
2. Toto opatření se použije obdobně též na jiné osoby než zaměstnance, které jsou povinny se jimi řídit na základě jiného právního titulu.

Čl. 2

Pojmy

Pro účely tohoto opatření se rozumí:

- technickým aktivem – hardware a software vybavení,
- důvěrností informací – zachování důvěrnosti spočívající v tom, že informace by měla být přístupná jen tomu, kdo je oprávněn se s ní seznamovat a nakládat,



PEDAGOGICKÁ
FAKULTA
Univerzita Karlova

- integritou informací – ujištění, že informace nebyly neoprávněně změněny, přičemž je chráněna jejich přesnost a úplnost,
- chráněnou informací – informace, která má pro chod univerzity zásadní význam a jejímž vyzrazením, zneužitím, zničením, ztrátou, neautorizovanou změnou nebo nedostupností by univerzitě mohla vzniknout újma, případně by mohlo dojít k ohrožení řádného plnění poslání univerzity,
- interní informací – informace, která není veřejně přístupná a je určena pro vnitřní potřebu fakulty, resp. univerzity,
- důvěrnou informací – chráněná informace nebo interní informace,
- informačním systémem (IS) – funkční celek zabezpečující cílené a systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací a dat, který zahrnuje datové a informační zdroje, nosiče, technické, programové a pracovní prostředky, technologie a postupy a související normy,
- kybernetickou bezpečností – souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru, jehož cílem je zajištění důvěrnosti, integrity a dostupnosti informací v kybernetickém prostoru,
- bezpečnostní událostí – událost, která může vyústit v bezpečnostní incident,
- bezpečnostním incidentem – narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb nebo bezpečnosti a integrity sítí elektronických komunikací, porušení bezpečnostních politik, bezpečnostních zásad nebo standardních bezpečnostních pravidel provozu informačních a komunikačních technologií,
- médiiem – externí paměťové zařízení typu USB flash disku, externího disku, nosiče CD a DVD a obdobná zařízení,
- mobilním zařízením – přenosný elektronický přístroj s operačním systémem, jako je mobilní telefon, notebook, tablet a obdobná zařízení,
- počítačovou sítí fakulty, resp. univerzity – soubor technických prostředků informačních a komunikačních technologií, a to včetně, nikoliv však výhradně, kabeláže, síťových prvků, serverů, počítačů, mobilních zařízení a jiných speciálních zařízení výpočetní techniky umožňujících zaměstnancům přístup k provozovaným službám v rámci fakulty/univerzity,
- vícefaktorovou autentizací (MFA) – ověřování pomocí dvou nebo více faktorů autentizace,
- uživatelským účtem – přístup zaměstnance do informačního systému, který odpovídá jeho pracovnímu zařazení a je definován unikátními přístupovými údaji,



PEDAGOGICKÁ
FAKULTA
Univerzita Karlova

- virtuální privátní sítě (VPN) – síť, která dovolí připojit vzdálené uživatele do cílené LAN přes Internet, kde je bezpečnost zajištěna pomocí šifrovaného tunelu mezi dvěma body navzájem,
- zařízením – technická zařízení ICT, jako jsou stolní počítače, notebooky, chytré telefony, tablety, tenci klienti, tiskárny nebo jiný specializovaný hardware včetně inteligentních měřičů a zařízení IoT,
- ICT útvarem – je na úrovni univerzity Ústav výpočetní techniky a na úrovni fakulty Středisko informačních technologií (dále jen „SIT“), jejichž agendou je správa prostředků ICT.

ČÁST DRUHÁ PRAVIDLA KYBERNETICKÉ BEZPEČNOSTI

Čl. 3

Pravidla kybernetické bezpečnosti

1. Za účelem zajištění kybernetické bezpečnosti jsou všichni zaměstnanci povinni dodržovat pravidla bezpečného chování při práci s informacemi v papírové a digitální podobě, při manipulaci s prostředky ICT nebo v rámci informačního systému stanovená tímto opatřením.
2. Zaměstnanci jsou dále povinni zejména:
 - ohlašovat prostřednictvím ohlašovacích kanálů kybernetické bezpečnosti události a incidenty, které by mohly narušit kybernetickou bezpečnost fakulty/univerzity,
 - v případě kontroly dodržování bezpečnostních pravidel poskytnout potřebnou součinnost.
3. Zaměstnanci jsou dále odpovědní za zabezpečení informací a služeb ve své působnosti a za tímto účelem se podílejí na zajišťování důvěrnosti, dostupnosti a integrity zpracovávaných informací a poskytovaných služeb.

Čl. 4

Bezpečné nakládání s aktivy

1. Zaměstnanci dbají na vhodné zabezpečení ICT prostředků, informací a dat před ztrátou, zneužitím, poškozením, odcizením nebo jiným ohrožením (dále jen „ohrožení“), a to jak v pracovní době, tak přiměřeným způsobem i v případě opuštění pracoviště.



PEDAGOGICKÁ
FAKULTA
Univerzita Karlova

2. Při opuštění pracoviště musí zaměstnanec vhodným způsobem zabezpečit veškeré písemnosti a média včetně přenosných médií, které obsahují důvěrné informace podle možností pracoviště tak, aby nebyly vystaveny možnosti snadného přístupu neautorizované osoby a nemohlo dojít k jejich ohrožení.

Čl. 5

Zabezpečení zařízení

1. Každé zařízení používané pro plnění pracovních povinností musí být zabezpečeno uživatelským heslem.
2. Zaměstnanec musí vypnout nebo uzamknout zařízení, pokud zůstává bez jeho dozoru.
3. Při práci na dálku jsou zaměstnanci povinni při ukončení činnosti se odhlásit od informačních systémů fakulty/univerzity, včetně vzdáleného přístupu přes virtuální privátní síť (VPN).
4. Zaměstnanec musí zajistit přiměřenou ochranu neobsluhovaných zařízení. Zaměstnanci jsou povinni po ukončení práce na zařízení provést odhlášení, a je-li to možné, zařízení fyzicky zajistit.
5. Vynášení zařízení mimo objekty fakulty je zakázáno, pokud přímo nesouvisí s výkonem pracovní činnosti.

Čl. 6

Přístupová hesla a vícefaktorová autentizace

1. V případě, kdy konkrétní systém umožňuje přihlašování prostřednictvím vícefaktorové autentizace (MFA), zajistí ICT útvar, který spravuje tento systém, aby zaměstnanci primárně využívali tuto metodu k přihlašování současně s přístupovým heslem.
2. K vícefaktorové autentizaci dle odstavce 1 může zaměstnanec užít vlastní zařízení za podmínek stanovených v článku 9 tohoto opatření děkana. V případě, že zaměstnanec nebude k tomuto účelu využívat vlastní zařízení, využije zařízení poskytnuté zaměstnavatelem.
3. Zaměstnanec postupuje v souladu s pravidly pro tvorbu a nakládání s přístupovými hesly a odpovídá zejména za zachování důvěrnosti vlastního hesla.
4. Zaměstnanec vytváří hesla a nakládá s nimi tak, že
 - udržuje unikátní heslo pro každé jednotlivé zařízení i jednotlivý informační systém a aplikaci,



PEDAGOGICKÁ
FAKULTA
Univerzita Karlova

- nepoužívá hesla využitá k soukromým účelům současně k uživatelským účtům fakulty/univerzity,
 - v heslu nepoužívá své jméno či příjmení, jméno či příjmení blízké osoby, datum narození a další informace, které se váží přímo k osobě zaměstnance a jsou obecně dostupné,
 - neukládá hesla na místech, kde by mohlo dojít k jejich krádeži či prozrazení,
 - neukládá hesla do webových prohlížečů v případě, že by k nim mohla získat přístup jiná osoba,
 - změni heslo
 - při prvním přihlášení do systému, pokud se nejedná o heslo, které si vytvořil sám, nebo
 - v případě důvodného podezření na jeho kompromitaci,
 - dodržuje minimální délku hesla 8 znaků a používá alespoň 3 z těchto kategorií komplexity hesla, nevyklučuje-li jejich užití systém, do něž má být heslo použito:
 - alespoň jedno velké písmeno (např. AKZSD),
 - alespoň jedno malé písmeno (např. bsdijsd),
 - alespoň jednu číslici (např. 7291), nebo
 - alespoň jeden speciální znak (např. „.“; „“; „@“; „#“; „%“; „!“; „\$“; „&“; „+“; „-“).
5. Pokud zaměstnanec nemá možnost pro konkrétní systém použít vícefaktorovou autentizaci (MFA), vytváří hesla dle odstavce 4 a navíc:
- nepoužívá předchozích 12 hesel,
 - měni heslo nejpozději každých 18 měsíců,
 - dodržuje minimální délku hesla 22 znaků jde-li o účet technických aktiv, 17 znaků jde-li o účet administrátora, a 12 znaků jde-li o účet uživatele, a zároveň používá všechny 4 z těchto kategorií komplexity hesla:
 - alespoň jedno velké písmeno (např. AKZSD),
 - alespoň jedno malé písmeno (např. bsdijsd),
 - alespoň jednu číslici (např. 7291) a
 - alespoň jeden speciální znak (např. „.“; „“; „@“; „#“; „%“; „!“; „\$“; „&“; „+“; „-“).
6. ICT útvar, který spravuje příslušný systém, zajistí, aby si zaměstnanec při nastavování hesla do systému nemohl nastavit heslo nesplňující požadavky na heslo k účtu uvedené v odstavci 4 a odstavci 5.



PEDAGOGICKÁ
FAKULTA
Univerzita Karlova

Čl. 7

Elektronická pošta

1. Zaměstnanci jsou povinni používat přidělený e-mailový účet pouze k plnění pracovních úkolů a zároveň nesmí využívat své soukromé e-mailové účty pro plnění pracovních úkolů. Automatické hromadné přeposílání pracovních zpráv na soukromé e-mailové adresy není dovoleno.
2. Je zakázáno registrovat a využívat e-mailovou adresu univerzity pro e-shopy, zasílání reklamních sdělení, newslettery a obdobné služby, pokud nesouvisí s výkonem práce. Uživatel odhlásí aktivní služby, které nesouvisí s účelem, pro něž mu byla e-mailová adresa přidělena, nepředstavuje-li to pro něj nepřiměřenou zátěž.
3. Při přijímání e-mailových zpráv dodržuje zaměstnanec bezpečnostní pravidla pro eliminaci podvodných e-mailů. Za tímto účelem
 - kontroluje skutečného odesílatele e-mailu, jestli vykazuje nestandardní syntaxi,
 - věnuje pozornost zprávám obsahujícím
 - významné gramatické chyby,
 - žádost o zadání nebo zaslání přístupových údajů,
 - žádost o druh finanční platby, nebo
 - žádost o zadání bankovních či osobních údajů, a
 - v případě podezření
 - neotvírá e-maily, jejichž obsah se jeví jako podezřelý, a neodpovídá na ně,
 - při otevírání souborů nepovoluje makra,
 - je-li to možné, ověřuje pravost e-mailu u odesílatele,
 - neotevívá podezřelé přílohy e-mailů, nevyplňuje a nekliká na aktivní okna nebo odkazy.

Čl. 8

Počítače, notebooky a jiná zařízení

1. Všechna zařízení, která jsou přidělena fakultou, musejí být začleněna do systému vzdálené správy, s výjimkou případů, kdy to není technicky možné.
2. V rámci užívání počítačů, notebooků a jiných zařízení přidělených fakultou zaměstnanec
 - brání v používání zařízení neautorizovaným a jiným osobám,
 - neprovádí svépomocí ani jinak servis a upgrade zařízení; tyto činnosti může provádět výhradně oprávněný pracovník SIT, nebo jiný zaměstnanec, který



PEDAGOGICKÁ
FAKULTA
Univerzita Karlova

má tuto činnost výslovně schválenou v rámci své pracovní role nebo na základě pověření vedení fakulty,

- neprodleně hlásí ztrátu zařízení svému vedoucímu zaměstnanci, a
 - nejméně jedenkrát do měsíce připojí zařízení do počítačové sítě univerzity, a to zejména za účelem provedení aktualizací, jedná-li se o mobilní zařízení.
3. Zařízení využívané pro výkon práce lze připojit pouze do zabezpečené sítě nebo při použití šifrovaného spojení prostřednictvím virtuální privátní sítě (VPN).

Čl. 9

Použití soukromého zařízení pro pracovní účely

Zaměstnanec, který používá pro pracovní účely soukromé zařízení, zajistí nebo nastaví na tomto zařízení:

- pravidelnou aktualizaci operačního systému zařízení a neprodlenou aktualizaci bezpečnostních aktualizací; používání zařízení s nepodporovanou verzí operačního systému se neumožňuje,
- aktivovaný a aktualizovaný firewall a bezpečný antivirový program,
- šifrování disku,
- automatické zamknutí zařízení nebo odhlášení,
- instalaci aplikací pouze z bezpečných ověřených zdrojů,
- nastavení vstupního bezpečného alfanumerického hesla, otisku prstu nebo identifikace pomocí rozpoznání obličeje, a
- ochranu proti úpravám snižujícím bezpečnost.

Čl. 10

Kopírky, tiskárny a skenery

Při provozu a používání tiskových, skenovacích, kopírovacích a obdobných zařízení je zakázáno nechávat bez dozoru zařízení při zpracovávání důvěrných informací.

Čl. 11

Média

1. Zaměstnanec je oprávněn užívat přenosná média a umísťovat na ně pracovní informace jen v případech, kdy je to nezbytné pro výkon práce, a odpovídá za bezpečnost těchto přenosných médií a jejich obsahu. V případě nalezení neznámého přenosného média je zakázáno toto médium připojovat do počítače, notebooku nebo jiného zařízení.



PEDAGOGICKÁ
FAKULTA
Univerzita Karlova

2. Zaměstnanec nesmí vynášet přenosná média mimo prostory univerzity, pokud to přímo nesouvisí s výkonem práce. V případě vynesení přenosného média mimo prostory univerzity musí zaměstnanec přenosné médium adekvátními prostředky zabezpečit proti krádeži a neoprávněné manipulaci s informacemi na médiu umístěnými. Média obsahující důvěrné údaje opatří zaměstnanec zejména šifrováním, případně dalšími vhodnými prvky ochrany.
3. V případě ztráty nebo odcizení média obsahujícího důvěrné informace nahlásí zaměstnanec tuto skutečnost bezpečnostnímu týmu počítačové sítě Univerzity Karlovy (CSIRT).

Čl. 12

Připojování zařízení do sítě univerzity

1. Připojovat jakékoliv zařízení do interních neveřejných sítí univerzity, resp. fakulty je povoleno pouze zaměstnancům SIT.
2. Přístup do sítě může být zaměstnanci zamítnut nebo omezen, pokud jeho zařízení nesplňuje podmínky stanovené tímto opatřením.

Čl. 13

Aktualizace software

1. Aktualizace softwaru provádí SIT zpravidla pomocí automatické instalace nebo ručně. Zaměstnanec poskytuje při provádění aktualizace nezbytnou součinnost.
2. Na zaměstnance využívající zařízení, která nejsou pod vzdálenou správou SIT, se povinnosti pro používání zařízení uvedené v článku 9 vztahují obdobně.

Čl. 14

Internet

1. Zaměstnanec nesmí na přiděleném zařízení přistupovat k těmto službám:
 - online hry,
 - pornografie a erotické stránky,
 - záměrné maskování identity zaměstnance zejména typu TOR,
 - P2P sítě za užití nástrojů zejména typu torrent, a
 - veřejná cloudová úložiště, která nejsou pod správou univerzity nebo univerzitního dodavatele takové služby.
2. Zaměstnanec nesmí na přidělené zařízení stahovat nebo jinak vkládat následující typy souborů:
 - aplikace a knihovny Windows (např. exe, dll),



PEDAGOGICKÁ
FAKULTA
Univerzita Karlova

- aplikace Unix,
 - instalační balíčky Unix/Linux (např. deb, rpm),
 - audio soubory (např. mp3, wav),
 - video soubory (např. avi, mp4, mpeg, mpg), a
 - soubory sítě Torrent.
3. Zákazy uvedené v odstavcích 1 a 2 neplatí v případech přímo souvisejících s výkonem pracovní činnosti.
4. Pracovníci SIT jsou oprávněni v souvislosti s aktuální bezpečnostní hrozbou omezit přístup k webovým stránkám a jiným ICT službám, jejichž prostřednictvím může být hrozba šířena.

Čl. 15

Vnitřní počítačová síť (LAN)

Zaměstnanci s přístupem do vnitřních sítí univerzity odpovídají za své činnosti prováděné v rámci těchto vnitřních sítí. Z důvodu zajištění bezpečnosti zaměstnanci, s výjimkou oprávněných zaměstnanců při výkonu práce, nesmí zejména

- zneužívat síťové prostředky pro osobní účely a zatěžovat kapacitu sítě,
- šířit škodlivý kód (malware),
- měnit síťové konfigurace koncových a síťových zařízení,
- využívat nástroje k záměrnému maskování identity,
- provádět skenování portů,
- provádět jakoukoliv formou monitorování počítačové sítě, které může vést k zachycení dat,
- obcházet autentizaci zaměstnance nebo obcházet zabezpečení jakéhokoliv zařízení, počítačové sítě nebo uživatelského účtu,
- provádět nepracovní aktivity na zařízeních univerzity, vedoucí k omezení nebo odepírání služeb jiným zaměstnancům,
- užívat programy, skripty nebo příkazy nebo zasílat zprávy s úmyslem omezit nebo znemožnit poskytování služeb nebo terminálových relací lokálně nebo přes počítačovou síť, internet nebo intranet,
- využívat bezpečnostních mezer nebo vytvářet útoky na komunikace v počítačových sítích, a
- předávat informace o konfiguraci a topologii sítě třetím osobám, nejde-li o případ, kdy tyto aktivity jsou součástí pracovních úkolů, kromě běžné obsluhy zasahovat do datových rozvodů.



Čl. 16

Ukládání, zálohování a archivace dat

Zaměstnanec ukládá soubory obsahující důvěrné informace pouze do oficiálně podporovaných nástrojů užívaných fakultou, resp. univerzitou do k tomu určených složek nebo informačních systémů fakulty, resp. univerzity, a to výhradně skrze účty přidělené fakultou/univerzitou.

Čl. 17

Navrácení aktiv

1. Zaměstnanec při skončení pracovněprávního vztahu navrátí či předá veškerá přidělená aktiva příslušné osobě ze SIT. To se týká zejména navrácení či předání
 - prostředků ICT,
 - identifikačních karet, čipů a dalších identifikačních a autentizačních prostředků,
 - software, licencí software, a
 - přístupových údajů ke službám, účtům a systémům.
2. Při změně pracovního zařazení zaměstnance se postupuje podle odstavce 1 přiměřeně.

Čl. 18

Nástroje pro vzdálenou komunikaci

1. Při komunikaci na dálku, zejména při uskutečňování audiovizuálních nebo audio hovorů, upřednostňuje zaměstnanec komunikační nástroje poskytnuté fakultou.
2. Zaměstnanec vhodným způsobem ověřuje identitu osob, se kterými vstupuje v komunikaci, a to zejména při sdílení důvěrných informací.
3. Při probíhajícím hovoru a případném sdílení informací je nutné sdílet pouze takové informace, které odpovídají pracovním potřebám a ke kterým mají účastníci odpovídající oprávnění přistupovat.

Čl. 19

Užívání nástrojů umělé inteligence

Zaměstnanci přistupují k používání nástrojů umělé inteligence s náležitou obezřetností a dbají na ochranu osobních údajů a důvěrných informací v souladu s právními předpisy a interními pravidly univerzity.



PEDAGOGICKÁ
FAKULTA
Univerzita Karlova

ČÁST TŘETÍ OHLAŠOVÁNÍ BEZPEČNOSTNÍCH UDÁLOSTÍ A INCIDENTŮ

Čl. 20

Ohlašování bezpečnostních událostí a incidentů

Bezpečnostní události a incidenty s dopadem na narušení kybernetické bezpečnosti musí uživatelé hlásit bezpečnostnímu týmu počítačové sítě Univerzity Karlovy (CSIRT) na e-mailovou adresu abuse@cuni.cz. Není-li možné ohlášení touto cestou, ohlásí se telefonicky na určeném telefonním čísle uvedeném na internetových stránkách univerzity.

ČÁST ČTVRTÁ ZÁVĚREČNÁ USTANOVENÍ

Toto opatření děkana nabývá platnosti a účinnosti dnem 2. června 2026.

V Praze dne 2. června 2026

prof. RNDr. Antonín Jančařík, Ph.D., v.r.
děkan fakulty