Česká zemědělská univerzita v Praze

Název předpisu	**Bezpečné chování uživatelů informačních systémů a výpočetní techniky**		
Druh předpisu	Směrnice rektora		
Pořadové číslo předpisu	**11/2023**	**Účinnost od**	11. 12. 2023
		Účinnost do	[Účinnost do]
Ve znění novely	Nerelevantní		
Stručný popis	Předpis vymezuje základní povinnosti uživatelů informačních systémů a výpočetní techniky ČZU za účelem zajištění minimálního standardu informační a kybernetické bezpečnosti.		
Odborný garant	OB - ředitel/ka		
Schválil	Nerelevantní	**Datum**	[Datum schválení]
Vydal	prof. Ing. Petr Sklenička, CSc., rektor	**Datum**	11. 12. 2023

Obsah

Směrnice rektora
Č. 11/2023

Bezpečné chování uživatelů informačních systémů a výpočetní techniky

Článek 1
Úvodní ustanovení

(1) Tato směrnice je platná pro Českou zemědělskou univerzitu v Praze a všechny její součásti (dále též jen „ČZU“) a stanovuje postupy bezpečného chování uživatelů informačních systémů a výpočetní techniky.

Článek 2
Pravidla pro bezpečné nakládání s informačními aktivy a zařízeními

(1) Uživatelé informačních systémů (dále též jen „IS“) či výpočetní techniky (dále též jen „ICT“) ČZU jsou povinni dodržovat zásady bezpečného zacházení se všemi daty a informacemi, které zpracovávají a ke kterým mají přístup, a bezpečně zacházet s dalšími jim svěřenými informačními aktivy.

(2) Uživatelé používají svěřená informační aktiva, IS, ICT a další zařízení výhradně k plnění svých pracovních či obdobných povinností. Každý uživatel je povinen se seznámit s pravidly a požadavky pro přístup a práci s infomačními aktivy, IS a ICT v rámci ČZU ihned po nástupu do pracovního poměru, po uzavření smluvního vztahu nebo po přijetí ke studiu.

(3) Uživatelé jsou povinni používat IS, ICT, mobilní zařízení, programové vybavení, informace a data podle pokynů a požadavků, které stanoví ČZU a komunikuje je prostřednictvím vedoucích zaměstnanců, Odboru bezpečnosti, Odboru informačních a komunikačních technologií, příp. dalších pověřených zaměstnanců ČZU, a které jsou dostupné uživatelům v písemné nebo elektronické formě pro bezpečné používání aplikací, informačních systémů, koncových zařízení a informací ČZU.

(4) Mezi základní povinnosti uživatelů patří zejména:

a. dodržovat stanovené bezpečnostní požadavky, zásady a pravidla ČZU stanovené v této směrnici a v dalších bezpečnostních dokumentech týkající se dílčích technologií a zařízení nebo interních předpisech ČZU;

b. uchovávat své autentizační údaje v tajnosti a nezpřístupňovat tyto autentizační údaje jiným osobám pro přístup do informačního prostředí a systémů a aplikací ČZU;

c. neprovádět důvěrné rozhovory na veřejnosti, sdílet interní nebo chráněné informace veřejným komunikačním zařízením nebo v prostředí, kde jsou neoprávněné osoby.

(5) Uživatelé jsou povinni dodržovat pravidlo tzv. „čistého stolu“ - nenechávat na svých pracovištích, pracovním stole a místech přístupných neautorizovaným osobám dostupné jakékoliv pracovní a chráněné informace, dokumenty či informační aktiva, pokud opustí své pracoviště. Veškeré pracovní a chráněné informace, data v jakékoliv podobě a aktiva vždy zabezpečí při odchodu z pracoviště proti narušení bezpečnosti informací, zneužití či zcizení podle interních pokynů a pravidel ČZU.

(6) Uživatelé jsou povinni také dodržovat veškeré bezpečnostní předpisy, opatření, pokyny, zásady bezpečného chování v kyberprostoru a řídit se dalšími bezpečnostními požadavky včetně aktivní účasti na zvládání kybernetických bezpečnostních incidentů.

(7) Uživatelé po vytištění dokumentů obsahujících osobní údaje nebo interní či chráněné informace musí bezodkladně odebrat vytištěné dokumenty z tiskárny nebo použít režim zabezpečeného tisku, pokud jej má tiskárna k dispozici. Chráněné informace mohou být kopírovány či tištěny pouze na zařízení s autentizací uživatele (PIN, čipová karta, …) nebo na zařízení umístěném v chráněném prostoru (kancelář, aj.).

(8) Uživatelé jsou povinni odebírat tiskové výstupy okamžitě po jejich vytištění. V případě, že při kontrole a odebírání vlastních tisků ze zařízení uživatel zjistí, že na zařízení zůstal jiný tiskový výstup a nemůže-li s jistotou určit jeho původce, jemuž by jej předal, provede jeho skartaci.

(9) Uživatelé jsou povinni používat uzamykatelné boxy a skříně pro uschování klasifikovaných osobních údajů a chráněných či interních informací a dat proti neautorizovanému přístupu osob k těmto informacím.

(10) Uživatel je povinen vrátit všechna svěřená a zapůjčená informační aktiva a prostředky v případě ukončení pracovního nebo smluvního poměru, a další svěřené ICT prostředky dle požadavků stanovených ve výstupním listu.

(11) Kopírky, tiskárny a scannery smí být uživateli používány výhradně k pořizování kopií v souvislosti s výkonem pracovní činnosti a v rozsahu nezbytném k zajištění těchto úkolů.

(12) Uživatelé mají zakázáno zasahovat do provozu kopírek, tiskáren a scannerů vyjma uživatelských úkonů (nastavení tisku, výměna toneru, zaseknutý papír apod.).

(13) Uživatel je povinen chránit přenosná paměťová média obsahující osobní údaje nebo interní či chráněné informace ČZU před ztrátou nebo krádeží (např. média bez dozoru ukládat na uzamčeném místě (skříň, kancelář, …), dbát zvláštní opatrnosti mimo prostory ČZU).

(14) Je zakázáno používat paměťová média z neznámých nebo nedůvěryhodných zdrojů (např. zapomenuté USB flash disky, neznámá CD/DVD, rozdávaná paměťová média).

Článek 3
Pravidla používání pouze legálního a schváleného HW a SW

(1) Uživatel smí používat pouze legálně zakoupený a schválený software v souladu s licenčními a právními požadavky pro používání SW.

(2) Uživatel smí používat pouze počítačové vybavení (HW), které mu bylo přiděleno nebo zapůjčeno prostřednictvím Odboru informačních a komunikačních technologií (dále jen „OIKT“), fakulty, nebo takový hardware, který je implicitně schválený, a tedy splňuje minimální bezpečnostní požadavky pro přístup k IS ČZU (např. aktualizovaný OS, antivirový SW atp.).

(3) Použití jiného HW a SW vybavení, které nebylo schváleno nebo přiděleno není uživatelům povoleno.

Článek 4

Požadavky na přístupová hesla (autentizační údaje) a jejich použití

(1) Politika stanovuje tyto základní požadavky na přístupová hesla do systémů a zacházení s nimi.

(2) ČZU stanovuje požadavky na silné (kvalitní) heslo:

a. minimální délka hesla musí odpovídat požadavkům a parametrům pro bezpečné přihlášení do IS a ICT, nebo informačního prostředí ČZU podle požadavků 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 jen “VoKB”). Detailní definice požadavků a parametrů na uživatelská hesla je uvedena v dokumentu rozhodnutí rektora – Řízení přístupu k informačním systémům;

b. heslo nesmí být snadno uhodnutelné, tj. není doporučeno používat obecně užívaná slova, vlastní jméno, příjmení nebo zkratky (v českém jazyce ani v jiné řeči), příp. jiné údaje ve vazbě na osobu uživatele, jeho rodinu, koníčky apod;

c. nesmí být použita hesla zaznamenaná ve veřejných databázích uniklých hesel;

d. uživatel nesmí tvořit hesla na základě mnohonásobně opakujících se znaků, přihlašovacího jména, e-mailu, názvu systému nebo obdobným způsobem.

(3) ČZU svými bezpečnostními opatřeními naplňuje obecné požadavky na bezpečné zacházení s hesly, jež odpovídají požadavkům VoKB.

(4) Zásady a požadavky, které je uživatel povinen dodržovat a respektovat:

a. chránit autentizační údaje proti zneužití (nesdělovat, nezapisovat, zabránit odpozorování);

b. důsledně odlišovat hesla pro pracovní a soukromé aplikace a systémy;

c. změnit heslo při každém podezření, že došlo k jeho prozrazení;

d. pro každou aplikaci a systém mít jiné heslo (pokud aplikace nevyužívá systém jednotného přihlášení);

e. není povoleno ukládání hesel pro další přihlášení (volba „Zapamatovat heslo“, “Remember password“) v běžných aplikacích, např. v internetovém prohlížeči;

f. hesla pravidelně obměňovat v požadovaném maximálním intervalu (pokud změna není vynucena systémy), přičemž toto pravidlo se nevztahuje na účty sloužící k obnově systému v případě havárie;

g. vyloučit opakování definovaného počtu předchozích hesel uživatele;

h. automatické zamykání účtu po definovaném počtu neplatných pokusů o přihlášení;

i. odblokování či resetování zapomenutého hesla do aplikace či systému pouze na základě interního postupu a pravidel ČZU.

(5) Uživatel je oprávněn pro zápis autentizačních údajů využívat pouze SW (např. správce hesel) schválený Manažerem kybernetické bezpečnosti (dále také jen „Manažer KB“).

(6) Uživatel je povinen zabezpečit autentizační prostředky proti ztrátě a odcizení (USB token, mobilní telefony, kam jsou zasílány SMS jednorázová hesla, čipy atd.).

(7) Uživatel je povinen bez prodlení nahlásit ztrátu svěřených informačních aktiv, zcizení nebo kompromitaci autentizačních údajů podle pravidel a požadavků směrnice rektora – Řízení a zvládání kybernetických bezpečnostních událostí a incidentů.

(8) Autentizační údaje pro privilegovaný přístup k systémům ČZU budou uloženy tak, aby byly dostupné v případě nouzových situací, a to bezpečným způsobem uložené v listinné (např. trezor, kde jsou uloženy obálky s vytištěnými hesly) nebo v elektronické (např. aplikace kde jsou uložená zašifrovaná hesla) podobě.

Článek 5
Bezpečné použití elektronické pošty a přístupu na internet

(1) Elektronickou poštu je uživatel oprávněn používat pouze pro pracovní činnosti, nikoliv pro soukromé aktivity a komunikaci.

(2) ČZU si vyhrazuje právo automaticky blokovat elektronickou poštu obsahující nepracovní informace, a to včetně příloh.

(3) Jsou blokovány spustitelné přílohy příchozích e-mailů a přílohy, které nelze zkontrolovat.

(4) Při používání a přijímání elektronické pošty musí uživatel dbát na dodržování základních principů bezpečnosti informací a chování v kyberprostoru, zejména při otevírání zpráv, které naplňují znaky podvodné zprávy a v případě, že obsahují přiložené soubory.

(5) Informace jsou předávány elektronickou poštou pouze v souladu s bezpečnostními opatřeními ČZU pro klasifikaci a ochranu informací pro zajištění důvěrnosti a integrity informací a dat (viz požadavky klasifikace a přípustného používání informačních aktiv ČZU).

(6) ČZU uplatňuje provozní a bezpečnostní pravidla a postupy pro zabezpečení elektronické pošty organizačními a technickými opatřeními jako např. filtrování vybraných příloh, omezení na maximální objem příchozí a odchozí pošty a velikosti elektronické schránky, příp. blokování odchozí komunikace v případě překročení těchto limitů.

(7) E-mailová komunikace je umožněna uživatelům pomocí schválené aplikace vzdáleného přístupu do poštovní schránky přes webové rozhraní.

(8) Uživatel má povinnost využívat automatické, nebo manuální archivace, smazání zpráv, ke zmenšení obsahu své e-mailové schránky.

(9) Není přípustné automatické přesměrování pracovní služební e-mailové adresy na externí a soukromé e-mailové adresy.

(10) Uživatelé elektronické pošty ČZU jsou povinni dodržovat při komunikaci interní zásady slušného chování, bezpečnostní požadavky a etická pravidla a další příp. doplňující pravidla a požadavky ČZU.

(11) Přístup k internetu (např. webovým stránkám, sociálním sítím) je povolen pouze k vykonávání pracovních činností. Explicitně je zakázáno navštěvovat internetové stránky s eticky nevhodným obsahem nebo odporující dobrým mravům.

(12) Je zakázáno obcházet nastavení připojení k internetu pomocí externích proxy serverů nebo jiných prostředků (např. anonymizérů) a připojovat se tak k internetu jiným než standardním způsobem.

(13) Je zakázáno ukládat či sdílet informace ČZU v prostředí internetu (např. cloudová uložiště) bez autorizovaného souhlasu odpovědné osoby ČZU. Uživatel konzultuje případné ukládání informací a jejich ochranu v prostředí internetu pro pracovní účely s Manažerem KB, nebo zástupcem Oddělení informační a kybernetické bezpečnosti Odboru bezpečnosti (dále jen „OIKB“).

(14) Je zakázáno stahovat spustitelné programy a soubory včetně her, šetřičů obrazovky atp.

(15) Je zakázáno používání veřejných sítí peer-to-peer pro sdílení (tzv. seed) souborů (např. Torrent).

(16) ČZU si vyhrazuje právo:

a. zakázat přístup k webovým stránkám s nepracovním a nevhodným obsahem;

b. monitorovat přístupy uživatelů na webové stránky.

c. regulovat dostupnost sítě internet jednotlivým uživatelům, korigovat jejích denní kapacitní limity přijatých a odeslaných dat z a do sítě internet.

Článek 6
Pravidla oprávněného a bezpečného užívání ICT

(1) Uživatel je povinen dodržovat všechny bezpečnostní předpisy, požadavky, opatření, pokyny a postupy stanovené pro používání svěřených IS a ICT tak, aby nedošlo k porušení bezpečnosti informací, nebo škodě příp. poškození nebo zničení informačních aktiv ČZU.

(2) Uživatelé využívají přidělené ICT prostředky a přístupy k ICT a IS ČZU pouze k výkonu svých pracovních povinností a ke své pracovní činnosti pro které jsou určeny.

(3) Uživatelům je zakázáno využívat prostředky ICT, které jsou majetkem ČZU nebo jsou součástí IS ČZU pro soukromou potřebu, nebo pro jakoukoliv neoprávněnou, neetickou či trestnou činnost.

(4) Přístup do sítě a k informacím je povolen pouze oprávněným uživatelům, kteří mají v rámci ČZU zřízen účet. Je zakázáno umožnit přístup do sítě a k informacím osobám, které účet zřízen nemají, nemají právo získat účet, nebo kterým byl účet zablokován, či zrušen.

(5) Uživatel je oprávněn používat pouze přístupová práva, která mu byla řádným způsobem přiřazena nebo mu náležejí dle přiřazené role (např. dle organizačního zařazení, pracovní pozice atd.), a není oprávněn vyvíjet žádnou činnost směřující k obejití tohoto ustanovení. Pokud uživatel jakýmkoliv způsobem získá přístupová práva, která mu nebyla přidělena (např. chybou programů nebo technického vybavení), je povinen tuto skutečnost neprodleně oznámit správci prostředků ICT, resp. Garantovi aktiva, příp. přímo Manažerovi KB. Takto získaná práva nesmí uživatel použít.

(6) Uživatel je oprávněn pracovat na ICT ČZU a v programovém vybavení (aplikacích) pouze pod svým uživatelským jménem a heslem jemu přiděleným. Uživatel zodpovídá za škody vzniklé v důsledku zneužití jeho účtu zaviněného nedbalou manipulací s uživatelským účtem.

(7) Uživatel je povinen při manipulaci s informacemi respektovat pravidla a požadavky jednotného zacházení s informacemi z hlediska důvěrnosti, která jsou definována tzv. klasifikační úrovní aktiv.

(8) Uživatel není oprávněn měnit, konfigurovat nebo opravovat svěřené prostředky a počítačové vybavení.

(9) Uživatel je povinen se chovat tak, aby jeho činnost v minimálním rozsahu negativně ovlivňovala možnosti využití prostředků ICT dalšími uživateli.

(10) Uživatel nemá právo instalovat či odinstalovat programové vybavení (SW), pokud není stanoveno jinak dalšími interní pokyny nebo návody OIKT (nebo OIKB) ČZU.

(11) Uživatelé používají získané informace a data z informačních systémů a aplikací ČZU pouze pro plnění svých pracovních povinností.

(12) Při zjištění porušení zásad a požadavků stanovených touto směrnicí, nebo při podezření ze zneužívání sítě ČZU, nebo přístupu k ICT nebo informací, je povinností uživatele okamžitě informovat odpovědného Garanta aktiv, vedoucího zaměstnance, resp. přímo Manažera KB v souladu s požadavky a pravidly směrnice rektora – Řízení a zvládání kybernetických bezpečnostních událostí a incidentů.

(13) Uživatel nemá právo vkládat do výpočetní techniky data nesouvisející s jeho pracovní činností.

(14) Uživatel nemá právo připojovat do prostředí ČZU žádnou výpočetní techniku, která nebyla implicitně schválena splněním minimálních bezpečnostních požadavků na ICT pro přístup k IS ČZU nebo dodána OIKT ČZU.

(15) Uživatelům je dále zejména zakázáno:

a. provádět jakoukoliv činnost, která by mohla ohrozit provozuschopnost nebo bezpečnost pracovní stanice nebo počítačové sítě, nebo IS a ICT a primárních aktiv ČZU;

b. obcházet bezpečnostní funkce prostředků ICT a programového vybavení;

c. vědomě používat v síti ČZU prostředky ICT nakažené škodlivými kódy;

d. přerušovat a bránit operačnímu systému a instalovanému SW v provádění automatických aktualizací;

e. přerušovat a bránit monitoringu využití PC ve sběru dat;

f. přerušovat a bránit antivirovému programu při kontrole systémů a provádění automatických aktualizací;

g. instalovat programy nebo technická zařízení, která monitorují činnost jiných uživatelů nebo serverů, případně jinak zasahují do oblasti sítě;

h. provádět technické zásahy do konfigurace zařízení sítě a pracovních stanic;

i. používat svěřené ICT jinak než k činnostem přímo souvisejícím s pracovní činností.;

j. provozovat činnosti související s možností neoprávněného proniknutí do ochrany místního nebo cizího počítačového systému nebo odhalení hesel jiných osob (nejen uživatelů místní sítě), uchovávat data nebo programy, které jsou k této činnosti určeny;

k. provádět jakékoli akce, které vedou k narušení dat jiného uživatele, a to i v těch případech, kdy uživatel svá vlastní data explicitně nechrání;

l. kopírovat jakákoliv data nebo programy z uživatelských adresářů bez souhlasu jejich vlastníků (to zahrnuje i samotné prohlížení těchto adresářů). Toto omezení platí i v případě, že uživatelské adresáře jsou svými majiteli ponechány volně přístupné elektronickými prostředky;

m. zveřejňovat informace či soubory dat, které by mohly vést k poškození dobrého jména ČZU, ochrany sítě, programů nebo ČZU. Za zveřejnění se považuje zejména jejich neautorizované zpřístupnění v jakékoli podobě a způsobem (v papírové nebo elektronické podobě);

n. manipulovat (přemísťovat, nastavovat, přenášet) s jednotlivými PC stanicemi a zařízeními;

o. znemožňovat správci ICT jakýmkoliv způsobem vzdálený přístup k prostředkům ICT.

(16) Uživatel je povinen zabránit neoprávněným osobám v odezírání obsahu obrazovky nebo zneužití IS a ICT ČZU.

(17) Uživatel je odpovědný za stav svěřeného ICT a je povinen s nimi nakládat v souladu s pokyny a postupy OIKT, příp. s příslušnou další dokumentací.

(18) Uživatelé nejsou oprávněni měnit ani jakkoliv zasahovat do nastaveného prostředí ICT, systémů a aplikací, zařízení, bezpečnostních SW a služeb nastavených administrátory ICT či provádět jejich odinstalování, nebo změnu, výjimkou je tzv. uživatelské nastavení např. definice hesla.

(19) Uživatel při informaci o dostupných aktualizacích operačního systému zbytečně neoddaluje jejich instalaci a umožní příslušnému zařízení provedení restartu v nejbližším možném termínu.

(20) Uživatel není v žádném případě oprávněn připojit k interní síti nebo výpočetní technice ČZU (notebooku, počítači, tabletu) jakékoli neznámé zařízení (nalezené USB disky apod.).

(21) Uživatelé jsou povinni dodržovat zásadu prázdné obrazovky, tj. uživatel je povinen zajistit, aby zařízení (počítač, tablet, notebook, mobilní telefon apod.), který nepoužívá a nemá ho pod kontrolou, byl buď vypnutý, nebo chráněný pomocí uzamčení obrazovky (např. pro operační systém Windows prostředí stiskem kláves Win+L případně Ctrl+Alt+Del a volbou „Uzamknout“).

(22) K hlášení chyb, problémů, zvláštního chování HW nebo SW a požadavků spojených s ICT prostředky je uživatel povinen použít aplikaci HelpDesk nebo kontaktovat telefonickou podporu OIKT nebo zaslat e-mail na generickou (centrální) e-mailovou adresu OIKT.

Článek 7
Bezpečný vzdálený přístup

(1) V případě přístupu uživatele k informačnímu systému ČZU z prostor mimo ČZU mohou být jeho přístupová práva omezena a mohou se lišit od standardních uživatelských práv při připojení ze standardního pracoviště, tj. přímo do počítačové sítě na pracovišti.

(2) Při vzdáleném přístupu osob podílejících se na provozu a správě informačních systémům ČZU bude prováděna identifikace a nejméně stejně silná autentizace jako při přístupu z vnitřní sítě.

(3) Každý vzdálený přístup uživatele musí být vždy schválen OIKB nebo Manažerem KB a evidován v aplikaci HelpDesk.

(4) Pro vzdálený přístup do sítě a k informačním aktivům ČZU je požadována min. dvou faktorová autentizace.

(5) Komunikace vzdáleného přístupu do prostředí ČZU musí být šifrována a umožněna jen autorizovaným osobám.

(6) Všechny autentizační metody použité pro přihlášení k informačním systémům ČZU a aplikacím ČZU, které jsou hodnoceny, jako klíčové nebo významné IS vyžadují minimálně dvou faktorovou autentizaci pro přístup do informačního prostředí a k aktivům ČZU.

(7) Osoby podílející se na provozu a správě informačních systémů budou používat pro vzdálený přístup k informačním systémům jen řádně zabezpečené prostředky (jinak jim nebude umožněn přístup do informačního prostředí ČZU).

(8) Zařízení pro vzdálený přístup musí být nakonfigurováno tak, že splňuje bezpečnostní požadavky a před přístupem k informacím uloženým v zařízení vyžaduje autentizaci.

Článek 8
Bezpečné chování na sociálních sítích

(1) Používání sociálních sítí (např. Facebook, Twitter, Instagram, apod) jménem ČZU je povoleno jen oprávněným zaměstnancům.

(2) Autentizační údaje pro správu profilů organizace na sociálních sítích budou uloženy tak, aby byly dostupné v případě nouzových situací, a to bezpečným způsobem v listinné podobě (např. trezor, kde jsou uloženy obálky s vytištěnými hesly) nebo v elektronické podobě (např. aplikace kde jsou uložená zašifrovaná hesla).

(3) Uživatelé nemají oprávnění používat pracovní e-mailovou adresu při komunikaci na sociálních sítích, kromě zaměstnanců ČZU, kteří toto mají povoleno v rámci výkonu svých pracovních činností. Uživatel vystupuje na sociálních sítích tak, aby svým chováním nepoškozoval dobré jméno ČZU a nepoškozoval cizí oprávněné zájmy, nebo nezpůsobil újmu cizím osobám.

(4) Uživatel je povinen přistupovat s nedůvěrou k tzv. hoaxům (poplašným smyšleným zprávám, obvykle konstruovaných tak, aby působily dojmem, že se skutečně udály) uvedených na sociálních sítích a informace si ověřovat z různých zdrojů nebo jinak prověřit.

Článek 9

Bezpečnost ve vztahu k mobilním zařízením

(1) Zaměstnanec ČZU jakožto uživatel zařízení, kterému byl svěřen přenosný počítač nebo zařízení (notebook, tablet, mobilní telefon) je povinen zajistit a vynaložit maximální péči a úsilí k tomu, aby svěřené zařízení nebylo odcizeno, poškozeno nebo zneužito.

(2) Každý uživatel je povinen při používání mobilních zařízení zachovávat bezpečnostní opatřením a pravidla, aby nedošlo ke kompromitaci informací, které na mobilním zařízení zpracovává nebo ukládá.

(3) Uživatel je povinen chránit data a informace ČZU uložené na mobilním zařízení v souladu s jejich bezpečnostní klasifikací a chránit mobilní zařízení proti malwaru.

(4) V případě ukládání interních či chráněných informací na mobilní zařízení musí být úložný prostor mobilního zařízení chráněn použitím vhodné kryptografické ochrany.

(5) Je zakázáno přenechávat mobilní zařízení k používání třetím osobám, včetně rodinných příslušníků.

(6) Uživatel není oprávněn měnit bezpečnostní nastavení svěřených mobilních zařízení, ani se je nesnažit obcházet.

(7) Je dovolen provoz mobilních zařízení pouze s výrobcem podporovaným operačním systémem.

(8) Přístup mobilního zařízení do sítě ČZU je podmíněn autorizací a autentizací uživatele a splněním minimálních bezpečnostních požadavků na ICT pro přístup k IS ČZU.

(9) Veškeré instalace, změny a aktualizace programového vybavení na svěřeném mobilním zařízení přistupujícím do počítačové sítě ČZU mohou být prováděny jen oprávněnými osobami.

   a. Uživatelé nejsou oprávněni na tato zařízení instalovat jakýkoliv SW, který nebyl schválený či povolený Manažerem KB nebo ředitelem OIKT.

   b. Je zakázáno provádět činnosti tzv. jailbreak (tj. proces, pomocí kterého jsou odebrána softwarová omezení v operačním systému iOS u mobilních telefonů Apple) a root zařízení (tj. proces, který umožňuje uživatelům chytrých telefonů, tabletů a dalších zařízení s operačním systémem Android přepnutí do tzv. privilegovaného režimu) na mobilních zařízeních.

(10) Uživatel není oprávněn na služebním telefonu vytvářet Wi-Fi hotspoty v budovách ČZU. Uživatel je při používání přenosného zařízení mimo prostory ČZU povinen v rámci možnosti zabránit tomu, aby informace při používání zařízení nebyly odpozorovány nebo odposlouchávány neoprávněnou osobou.

(11) Uživatel je povinen zabezpečit svěřené mobilní zařízení (telefon, tablet), a to tak, že má nastavený časový zámek s číselným kódem, heslem, nebo i jiné způsoby zabezpečení pro

odemknutí obrazovky (např. biometrický zámek). Zařízení se po uplynutí časového intervalu automaticky uzamkne proti použití v případě jeho nepoužívání a nečinnosti.

(12) Před vyřazením mobilního zařízení či při ukončení pracovního poměru zaměstnance musí být data na mobilním zařízení smazána a zařízení uvedeno do továrního nastavení.

(13) ČZU je oprávněna na svěřeném zařízení instalovat a aktivovat funkce pro detekci polohy zařízení a dálkové smazání obsahu. Tyto funkce mohou být využity pouze v případě ztráty zařízení hlášené zaměstnancem.

Článek 10

Bezpečnostní pravidla fyzické ochrany svěřených prostředků

(1) Uživatel má povinnost chránit svěřené ICT před ztrátou, poškozením, zničením či odcizením přiměřenými prostředky.

(2) Uživatel nikdy nenechává v automobilu nebo v jakémkoli veřejném prostoru (např. restauraci) bez dozoru mobilní telefon, notebook, ani jiné zařízení, které využívá pro práci.

(3) Uživatel je povinen dbát na to, aby výpočetní technika a svěřené prostředky nebyly umístěné v blízkosti zdrojů tepla a vlhkosti, které by je mohly poškodit, ani jinak znemožnit funkčnost a bezpečnost svěřených prostředků.

(4) Uživatel je povinen zabezpečit ICT prostředky a příp. další aktiva (např. písemnosti) do uzamykatelných skříněk či prostoru pro zabezpečení neautorizovaného přístupu osob či zneužití prostředků.

(5) Uživatel v případě jakékoliv pochybnosti o použití vhodného bezpečnostního opatření je povinen kontaktovat OIKB nebo Manažera KB ČZU.

(6) Uživatel je povinen neprodleně nahlásit ztrátu nebo krádež svěřeného zařízení prostřednictvím systému helpdesk nebo na e-mail bezpecnost@czu.cz, v souladu s postupy a pravidly směrnice rektora – Řízení a zvládání kybernetických bezpečnostních událostí a incidentů.

Článek 11

Závěrečná ustanovení

Tato směrnice nabývá platnosti a účinnosti dnem vyhlášení.

V Praze dne 11. prosince 2023

prof. Ing. Petr Sklenička, CSc.
rektor, *v. r.*