Jihočeská univerzita v Českých Budějovicích

Označení dokumentu:	**ISMS-S-001**
Název dokumentu:	**Práce na dálku**
Typ dokumentu:	Interní směrnice JU
Rozsah:	Směrnice se týká všech zaměstnanců JU, kteří žádají o práci na dálku a využívají pro vykonání své pracovní činnosti technické zařízení, které je ve vlastnictví JU.
Prvek legislativy:	Opatření rektora 530
Datum vydání:	25. 09. 2023
Datum účinnosti:	**25. 09. 2023**
Platnost do:	odvolání
Počet stran + příloh:	4 + 1
Verze:	1.0
Význam a benefity:	Význam směrnice je zabezpečení dat při činnosti zaměstnanců v režimu práce na dálku a stanovení požadavků na bezpečný přístup do sítě JU z externího pracoviště.
Uložení:	Portál ISMS JU – https://isms.jcu.cz
Ruší dokumenty:	ISMS-010_Homeworking + přílohy
Zpracovatel:	Jan Urbánek - Manažer KB JU
Přezkoumal:	Výbor pro kybernetickou bezpečnost JU
Schválil:	Výbor pro kybernetickou bezpečnost JU

Informační vyhlášení

Před zahájením práce na dálku musí být zaměstnanci JU tato forma činnosti prokazatelně povolena. Pro dodržení postupu jejího schvalování je nutno respektovat Opatření rektora k výkonu práce zaměstnanců Jihočeské univerzity v Českých Budějovicích mimo pracoviště zaměstnavatele – práce na dálku R530 ze dne 29. 9. 2023

a) Žádost a její schválení

Zaměstnanec ve své písemné žádosti zdůvodní potřebu práce na dálku, a pokud mu bude jeho nadřízeným potvrzena, musí ji schválit vedoucí. V konečné fázi před zahájením práce na dálku musí být vyplněn a personálnímu útvaru předán formulář *ISMS-S-001_Prace_na_dalku_povoleni* (příloha 1 této směrnice), potvrzený příslušnými pracovníky dané součásti JU (rektor/děkan, vedoucí úseku/útvaru, nadřízený, technik BOZP).

b) Připojení k síti JU

JU nezajišťuje zřízení konektivity pro zaměstnance / uživatele pracujícího na dálku. Nejdříve je nutné zajistit si připojení externího pracoviště k internetu a pak přístup přes VPN koncentrátor do sítě JU. Jde o šifrované připojení do interní sítě JU s přístupen přes internet pod IP adresou JU.

1. **Přístup do sítě JU**

Aby mohl uživatel, co pracuje na dálku, přistupovat k vybraným serverům JU anebo univerzitním informačním systémům (IS), jako např. FIS, MIS, STAG, EGJE atd., musí být splněny tyto podmínky:

I. Jeho počítač musí mít aktivní připojení k internetu a nainstalovaný VPN koncentrátor zvolený správcem VPN JU[1];

II. Musí mít vytvořený univerzitní účet a nastavené freeradius heslo. K tomu je třeba se přihlásit svými univerzitními přihlašovacími údaji do služby IDM (https://idm.jcu.cz) a zvolit "Změna hesla freeradius";

c) Pravidla bezpečnosti IT

1. **Co musí uživatel v režimu práce na dálku dodržovat**

- Přístup k informačním systémům na JU realizuje uživatel vždy jen prostřednictvím šifrovaného VPN spojení;
- po schválení žádosti o práci na dálku musí uživatel nejprve projednat možnosti přístupu a parametry připojení k předem schváleným službám ICT JU s IT manažerem své součásti, který podle potřeby spolupracuje se správci systémů;

[1] Detailní popis a návody tohoto procesu lze nalézt na http://vpn.jcu.cz.

- v případě, že bude uživatel vzdáleně přistupovat k celouniverzitním informačním systémům a bude potřebovat odbornou pomoc, obrátí se na HelpDesk těchto IS na adrese: *https://servicedesk.jcu.cz*;
- firemní počítač, který bude používán při práci na dálku musí být zkontrolován správcem IT součásti a vybaven nezbytným softwarem chránícím před neoprávněným přístupem z internetu a před zavlečením škodlivého kódu nebo dalších bezpečnostních programů;
- přístup na firemní počítač musí být zajištěn uživatelským účtem a heslem a tyto autentizační údaje je třeba chránit proti zneužití;
- uživatel pracující vzdáleně, je povinen výsledky své práce zálohovat a zálohy neprodleně ukládat buď na externí médium nebo na určený server v síti JU (po dohodě se správcem IT své součásti);
- má-li uživatel v IDM zaznamenánu svoji privátní e-mail adresu, která nemá doménu jcu.cz, musí ji v této databázi udržovat aktuální a plně funkční, aby mohla být využívána k oboustranné komunikaci mezi ním a JU.

2. Uživatel pracující na dálku <u>nesmí:</u>

- na počítači vlastněný JU provádět nelegální činnosti, např. stahování nepovoleného obsahu (hudba, videa, …) z internetu apod.;
- nesmí využívat počítač JU k osobním komerčním účelům (poskytovat informace, programy či data za úplatu apod.);
- svěřené prostředky ICT (počítač, tiskárnu a příslušenství) nesmí zpřístupnit jiným osobám (např. rodinným příslušníkům);
- počítač používaný pro práci na dálku (je-li přenosný), nesmí být ponechán v automobilu či jinde mimo externí pracoviště bez zvýšeného dohledu;
- nesmí se připojovat s firemním počítačem na nezabezpečené (bez hesla) bezdrátové přístupové body – typicky FreeWiFi v restauracích, na hotelech, letištích a jiných lokalit.
- dále se uživatel řídí bezpečnostními politikami ISMS JU a směrnic k nim sdružených, které jsou dostupné na webu https://isms.jcu.cz.

d) Software a Hardware

1. Software

Uživatel smí používat při své práci pouze legální software s přidělenou licencí JU nebo freeware a současně dodržovat jimi definované licenční podmínky.

V systému počítače musí být instalovány bez zbytečného prodlení opravné balíčky (automatická aktualizace) vydané výrobcem operačního systému a dalších SW aplikací na něm instalovaných.

2. **Hardware**

Uživatel, co pracuje na dálku, není oprávněn zasahovat do HW konfigurace a BIOSu počítače dodaného JU bez předchozího souhlasu svého nadřízeného a správce IT své součásti.

3. **Opravy a servis svěřených zařízení**

Závady SW a HW hlásí zaměstnanec správci IT své součásti. V případě, že nelze problém vyřešit vzdáleně, může být zaměstnanec vyzván, aby počítač dopravil na stanovené místo dle dohody.

e) Ochrana informací

Uživatel v režimu práce na dálku nesmí šířit chráněné informace JU (veškeré informace a údaje, které je nutné ochraňovat před přístupem nepovolaných osob) či umožnit jejich zneužitím jinou stranou. Jde např. o obchodní smlouvy, know-how, provozní metody, procedury, pracovní postupy, koncepce, strategie a osobní údaje ve smyslu zákona č.110/2019 Sb. a pozdějších předpisů apod. Uživatel musí dodržovat autorský zákon a všechny právní předpisy související s ochranou informací.

Bude-li zaměstnanec přistupovat k citlivým osobním údajům – studentů, zaměstnanců, partnerů a firem spolupracujících s JU, dle výše zmíněného zákona, ev. jiným citlivým datům JU a tato data bude přenášet a ukládat na své PC, je nutné je zašifrovat.

ICT prostředky svěřené do užívání pro práci na dálku musí uživatel chránit proti poškození a zneužití a zacházet s nimi dle návodu výrobce a rad nebo nařízení správce IT své součásti.

f) BOZP a PO

Zaměstnanec JU provozující práci na dálku musí dodržovat stejná pravidla a pokyny týkající se bezpečnosti ochrany zdraví při práci a požární ochrany jako by pracoval v normálním režimu na JU. Byl poučen technikem BOZP a PO JU a toto stvrdil svým podpisem při sjednání pracovního poměru na JU. O případných změnách v souvisejících zákonech bude zaměstnanec informován e-mailem.

Činnost v režimu práce na dálku smí být zahájena až po provedení zmíněného poučení a potvrzení přílohy č.1 této směrnice *ISMS-S-001_Prace_na_dalku_povoleni* spolu se schválením ostatními pracovníky, jejichž potvrzení je vyžadováno.

V případě kontroly dodržování opatření k zajištění BOZP a PO ze strany JU musí uživatel práce na dálku umožnit referentu BOZP a PO JU vstup do jeho domácího prostředí dle předem dohodnutých podmínek.