

# Bezpečná práce na dálku

## TIPY A DOPORUČENÍ

### PRO FIRMY



### Nastavte korporátní strategie a postupy (ideálně v předstihu)

Zajistěte jasnou strategii práce na dálku, včetně pokynů, jak přistupovat ke korporátním zdrojům a koho kontaktovat při problémech. Nastavte jasný postup pro případ, že se vyskytne bezpečnostní událost. Aplikujte zvláštní opatření na dokumenty pro střední a vrcholový management, zejména vyžadujících jejich souhlas, odezvu, informaci a podpisy.

### Zabezpečte svá zařízení pro práci na dálku



Zaveďte opatření jako šifrování disků, vypínání při nečinnosti, clony pro soukromí, mohutné nástroje pro ověřování a řízení vyměnitelných medií a šifrování (například pro USB disky). Nastavte proces pro znemožnění přístupu k zařízení, které se ztratilo nebo bylo ukradeno.



### Bezpečný vzdálený přístup

Není dovoleno, aby se zaměstnanci připojovali do korporátní sítě jinak než přes firemní VPN a za použití vícenásobného ověřování. Je nutné zajistit, aby se práce na dálku automaticky vypínala po stanovené době nečinnosti a bylo nutné nové ověřování.

### Operační systém a aplikace musí být stále aktualizovány



Tak se zmenší riziko, že kyberzločinci využijí neaktualizované zranitelnosti.



### Zabezpečte své korporátní komunikace

Vynucujte používání vícenásobného ověřování pro přístup ke korporátní elektronické poště. Zaměstnanci musí mít dostupnou zabezpečenou komunikaci jak mezi sebou, tak s vnějším světem.



### Zvyšujte povědomí zaměstnanců o rizicích práce na dálku

Poučujte zaměstnance o firemní strategii pro práci na dálku. Věnujte se zvýšení povědomí o kybernetických hrozbách, jako zejména phishing a sociální inženýrství.

### Pravidelně komunikujte se zaměstnanci



Dávejte realistické cíle, pracovní časové plány a navazující mechanismy. Tam kde je to možné buďte flexibilní i s ohledem na osobní situaci.

# Bezpečná práce na dálku

## TIPY A DOPORUČENÍ PRO ZAMĚSTNANCE



### Přístup k firemním údajům s použitím korporátních zařízení

Používejte pouze zařízení a software poskytnuté firmou. Vytvořte silná hesla (za použití zabezpečených nebo autorizovaných správců hesel, pokud jsou k dispozici), nezapisujte si je, a chraňte je před cizími, když je vkládáte. Neobcházejte doporučené přístupy, i když jsou zdánlivě jednodušší.

### Počkat. Přemýšlet. Připojit se.



Před započítím práce na dálku se seznamte s firemními zařízeními, zásadami a postupy firmy. Ujistěte se, že zařízení rozumíte, víte co dělat a na koho se obrátit pro pomoc.



### Bezpečný vzdálený přístup

Připojíte se do korporátní sítě pouze přes korporátní VPN a chraňte si své doklady-tokeny (například chytré karty) nutné pro VPN připojení.

### Chraňte si svá zařízení pro práci na dálku a pracovní prostředí



Nedovolte rodinným příslušníkům přístup k zařízením pro práci. Vypněte je a uzavřete kdykoli jsou mimo dohled a vždy je chraňte v bezpečí tak, aby se zabránilo ztrátě, poškození nebo krádeži. Nedovolte, aby Vám někdo koukal přes rameno, používejte clony a obrazovky nesměřujte na okna či do kamery.



### Ohlášení

V případě, že zjistíte jakoukoli neobvyklou nebo podezřelou činnost na jakémkoli zařízení pro Vaši práci na dálku, ihned se dohodnutým způsobem spojte se zaměstnavatelem.



### Bud'te pozorní

Dávejte si pozor na jakoukoli podezřelou činnost a žádosti, zejména finanční. Může to být obchodní počítačový podvod! V případě pochyb žádejte potvrzení od žadatele. Nepoužívejte odkazy nebo přílohy v nevyžádané elektronické poště a sms.

### Nesdílejte důvěrné a citlivé osobní informace



Nikdy neuvádějte osobní informace ve zprávách, i když zprávy vypadají jako legitimní. Raději se spojte přímo se zdrojem a žádejte potvrzení.



### Hledejte nové postupy

Přehodnoťte pracovní plány s přímými nadřízenými a členy týmu po dobu práce na dálku a to včetně rozdělení úkolů, termínů a komunikace.

### Užívání soukromých zařízení



Jesliže jedinou možností je užívání soukromých zařízení, a zaměstnavatel to dovoluje, musí být operační systém a software aktualizovány, včetně softwaru pro antivirus/antimalware, a spojení musí být zabezpečeno přes server VPN schválený firmou.



### Oddělujte práci a zábavu

Nepoužívejte zařízení pro práci na dálku k osobním účelům.