Biztonságos távmunka

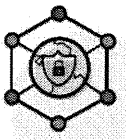
TIPPEK és TANÁCSOK MUNKAVÁLLALÓKNAK

Vállalati adatok elérése céges eszközökkel

Kizárólag a vállalat által biztosított eszközöket és szoftvereket használjon! Alkalmazzon erős jelszavakat (megbízható/jóváhagyott jelszókezelő alkalmazásokkal), amelyeket ne írjon le sehova, és ügyeljen arra is, hogy senki ne lássa, amikor a billentyűzeten beírja azokat! Tartózkodjon a megkerülő megoldásoktól, még akkor is, ha azok látszólag csak a szükséges szolgáltatásokat nyújtják!

Álljon meg! Gondolja át!

Mielőtt elkezdené a távmunkát, ismerkedjen meg a vállalati eszközökkel és előírásokkal! Bizonyosodjon meg róla, hogy tisztában van az eszközök használatával, mit tehet és mit nem használatuk során, és szükség esetén kihez fordulhat segítségért!



Tegye biztonságossá a távoli hozzáféréseket!

A vállalati hálózathoz csak a céges VPN-en keresztül csatlakozzon, és ügyeljen az ilyenkor használatos tokenek (pl. okoskártyák) védelmére!

Védje a távmunkára használt eszközeit és munkakörnyezetét!

A családtagok számára ne engedjen hozzáférést a munkaeszközeihez! Amikor az eszközöket felügyelet nélkül hagyja, mindig zárolja vagy kapcsolja ki őket annak érdekében, hogy megelőzze elvesztésüket, megrongálódásukat vagy ellopásukat. Védje képernyőjét a megfigyeléstől, monitorja ne nézzen az ablakra!

Jelentse be!

Amennyiben bármilyen szokatlan vagy gyanús aktivitást észlel bármelyik távmunkára használt eszközén, azonnal lépjen kapcsolatba a munkáltatójával a megfelelő csatornákon!

Maradjon éber!

Legyen figyelmes a gyanús eseményekre és üzenetekre, különösen, ha ezek pénzügyi vonatkozásúak! Ha kétsége támad, inkább duplán ellenőrizze az üzenet hitelességét a küldő felhívásával! Ne kattintson olyan e-mail és SMS hivatkozására, csatolmányára, amely érkezését nem várta!

Kerülje a bizalmas információk megosztását!

Válaszüzeneteiben soha ne adjon meg személyes információkat, még akkor sem, ha a kapott üzenet látszólag legitim forrásból származik! Ehelyett vegye fel a kapcsolatot közvetlenül az adott üzleti partnerrel, hogy ellenőrizze a kérés hitelességét!

Alakítsanak ki új rutinokat!

Egyeztesse a közvetlen vezetőséggel és a munkatársakkal a távmunka időszakára érvényes eljárásrendet, beleértve a feladatok kiosztását, a határidőket és a kommunikációs csatornákat!

Saját eszközök használata

Amennyiben saját eszközének használata az egyetlen lehetőség, és ehhez a munkáltató is hozzájárul, bizonyosodjon meg róla, hogy az eszköz operációs rendszere és a szoftverek naprakészek, van vírusirtó program telepítve és a hálózati kapcsolat a céges VPN-en keresztül biztosított!

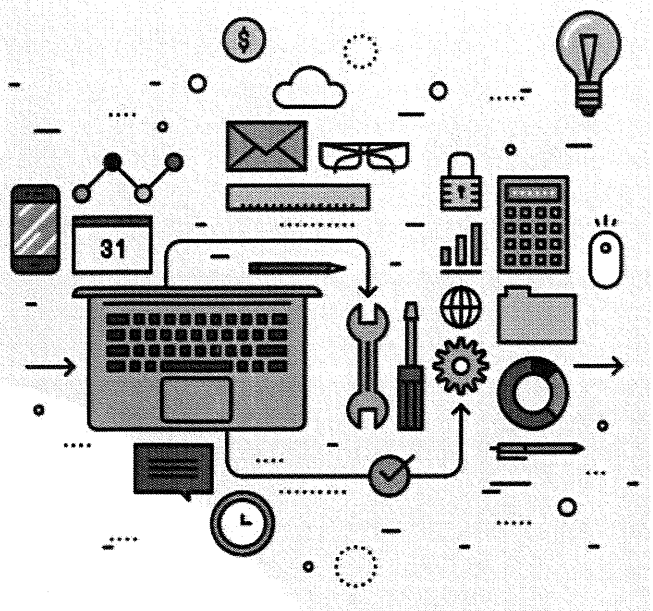
Válassza külön a munkaidőt és a pihenőidőt!

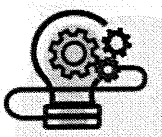
Kerülje a távmunkára szolgáló eszköz magáncélú használatát!

EUROPOL | EC3 European Cybercrime Centre

Biztonságos távmunka

TIPPEK és TANÁCSOK VÁLLALATOKNAK



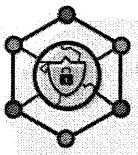


Hozzanak létre vállalati irányelveket és eljárásrendeket!

A távmunkával kapcsolatban határozzanak meg egyértelmű irányelveket, többek közt a vállalati eszközökhöz történő hozzáférésekre vonatkozóan, illetve, hogy kihez lehet fordulni probléma esetén! Biztonsági események bekövetkezésére írjanak elő egyértelmű eljárásrendet! Alakítsanak ki egyértelmű szabályokat a dokumentumok jóváhagyására, a visszacsatolásra és a tájékoztatásra!

Tegyék biztonságossá a távmunkához használt eszközöket!

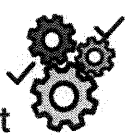
Alkalmazzanak olyan megoldásokat, mint például a merevlemez-titkosítás, az inaktivitás miatti időtúllépés, a betekintésvédelmi szűrők, erős hitelesítés, valamint a cserélhető adathordozók (pl.: USB meghajtók) felügyelete és titkosítása! Tegyék lehetővé, hogy az ellopott, elhagyott eszközökhöz való hozzáférés távolról is letiltható legyen!



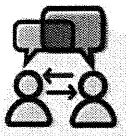
Tegyék biztonságossá a távoli hozzáférést!

Az alkalmazottak számára kizárólag vállalati VPN-hálózaton keresztül, többlépcsős hitelesítéssel engedélyezzék a vállalati hálózathoz történő csatlakozást! Állítsanak be automatikus időtúllépési korlátot a távoli munkamenetek számára, illetve meghatározott idejű inaktivitás esetén kényszerítsék ki a hitelesítő adatok ismételt megadását!

Tartsák naprakészen az eszközök operációs rendszerét és az alkalmazásokat!



Ez segíthet csökkenteni annak kockázatát, hogy a kiberbűnözők a javítatlan sérülékenységeket kihasználják.



Tegyék biztonságossá a vállalati kommunikációt!

Tegyék kötelezővé a többfaktoros hitelesítés használatát a vállalati e-mail fiókok eléréséhez! Gondoskodjanak biztonságos kommunikációs csatornákról, hogy az alkalmazottak könnyen elérhessék egymást és a külső partnereket!

Fokozzák a biztonsági monitorozást!

Aktívan ellenőrizzék a szokatlan távoli felhasználói tevékenységeket, és emeljék a VPN-nel összefüggő támadások figyelmeztetési szintjét!

Tájékoztassák az alkalmazottakat a távmunkából adódó kockázatokról!

Ismertessék az alkalmazottakkal a vállalat távmunkára vonatkozó irányelveit! Szánjanak időt arra, hogy felhívják az alkalmazottak figyelmét a számítógépes fenyegetésekre, különösen az adathalász és a pszichológiai manipulációs támadásokra!

Rendszeresen ellenőrizzék a beosztottakat!

Határozzanak meg reális célokat, munkaterveket és feladatok nyomonkövetésére szolgáló megoldásokat! Ahol lehetséges, legyenek rugalmasak, és vegyék figyelembe a személyes körülményeket!

EUROPOL | EC3 European Cybercrime Centre