					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P09S					Dokumentum címe: **Távmunka-szabályzat**							
Verzió: 1.0		Hatálybalépés dátuma: 01.01.2025			A dokumentum tulajdonosa:							
X	Szabályzat		Szabvány		Eljárás		Űrlap		Nyilvántartás		Egyéb	

Felülvizsgálati előzmények				
Felülvizsgálat száma	**Felülvizsgálat dátuma**	**Változások**	**Felülvizsgálta**	**A folyamat tulajdonosa**

Jóváhagyások			
Név	**Beosztás**	**Dátum**	**Aláírás**

Az alkalmazandó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	6.1., 6.2., 8. pont	
ISO/IEC 27002:2022	6. kontroll	
NIST SP 800-53 Rev.5	AC-17, AC-2	
EU NIS2	21. cikk (2) bekezdés b), 21. cikk (2) bekezdés h)	EU NIS2
EU DORA	9. cikk	EU DORA
COBIT 2019	DSS05, APO13	COBIT 2019
EU GDPR	32. cikk	EU GDPR

1. Cél

1.1 Jelen szabályzat meghatározza a távmunkában dolgozó munkavállalókra és szerződéses közreműködőkre vonatkozó biztonsági követelményeket, ideértve az otthoni munkavégzést, a megosztott munkaterületen végzett munkát és az utazás közbeni munkavégzést is.

1.2 Célja a vállalat által nem felügyelt környezetekből elért üzleti információk bizalmasságának, sértetlenségének és rendelkezésre állásának védelme.

1.3 Jelen szabályzat biztosítja a vonatkozó nemzetközi szabványoknak való megfelelést, valamint csökkenti a jogosulatlan hozzáférésből, adatvesztésből és szolgáltatáskiesésből eredő kockázatokat.

2. Hatály

2.1 Jelen szabályzat minden olyan munkatársra vonatkozik, beleértve a munkavállalókat, szerződéses közreműködőket, tanácsadókat és ideiglenes munkavállalókat, akik a vállalati telephelytől eltérő helyszínről érik el a vállalat rendszereit, hálózatait vagy adatait.

2.2 A szabályzat az alábbiakra terjed ki:

2.2.1 a vállalat által biztosított rendszerek és a saját tulajdonú eszközök használata

2.2.2 hozzáférés VPN-en, távoli asztali kapcsolaton vagy felhőszolgáltatásokon keresztül

2.2.3 az információk biztonságos kezelése a vállalati telephelyen kívül

2.2.4 nyomon követés, kivételkezelés és érvényesítés

2.3 A szabályzat a teljes munkaidős és részmunkaidős távmunkára egyaránt vonatkozik, ideértve az eseti távoli hozzáférést is.

3. Célkitűzések

3.1 A vállalati rendszerekhez vagy érzékeny adatokhoz való jogosulatlan hozzáférés megelőzése távmunkavégzés során.

3.2 Annak biztosítása, hogy az irodán kívül használt eszközök és kommunikációs kapcsolatok megfeleljenek az előírt biztonsági alapkövetelményeknek.

3.3 A távoli hozzáférési jogosultságok és a nyomon követés feletti kontroll fenntartása.

3.4 Egyértelmű iránymutatás biztosítása a munkavállalók és a vezetők számára a biztonságos távmunkavégzési gyakorlatokra vonatkozóan.

3.5 Megfelelés biztosítása az ISO, a NIS2, a GDPR, a DORA és a COBIT távoli és mobil munkavégzésre vonatkozó elvárásainak.

4. Szerepkörök és felelősségi körök

4.1 Ügyvezető

4.1.1 Jóváhagyja a távmunkavégzési megállapodásokat, és nyomon követi a megfelelést.

4.1.2 Eszkalálja a biztonsági incidenseket vagy az ismétlődő nemmegfelelőségeket.

4.1.3 Felülvizsgálja a kivételeket, és biztosítja az incidensek utókövetését.

4.2 IT-támogatás vagy kiszervezett informatikai szolgáltató

4.2.1 Biztonságos távoli hozzáférést alakít ki és tart fenn (pl. VPN, többtényezős hitelesítés).

4.2.2 Érvényesíti a végpontvédelmi, titkosítási és eszközkonfigurációs követelményeket.

4.2.3 Támogatja a felhasználókat, és kivizsgál minden technikai biztonsági problémát.

[... A 4.3–8. szakaszok nem szerepelnek ebben az előnézetben. A teljes tartalom eléréséhez vásárolja meg a teljes dokumentumot. ...]

9. Felülvizsgálati és frissítési követelmények

9.1 Éves szabályzat-felülvizsgálat

9.1.1 Az ügyvezetőnek és az IT-támogatásnak évente felül kell vizsgálnia jelen szabályzatot annak érdekében, hogy az összhangban maradjon a technológiai, munkaerővel kapcsolatos és jogi változásokkal.

9.2 Soron kívüli frissítést kiváltó okok

9.2.1 Azonnali felülvizsgálat szükséges az alábbi esetekben:

9.2.1.1 jelentős, távmunkával kapcsolatos biztonsági incidens

9.2.1.2 a NIS2, a GDPR vagy a DORA követelményeinek változása

9.2.1.3 új távoli hozzáférési technológiára történő átállás, például eltérő VPN-platform bevezetése

9.3 Verziókezelés és archiválás

9.3.1 Jelen szabályzat minden verzióját:

9.3.1.1 dátummal kell ellátni, és az ügyvezetőnek jóvá kell hagynia

9.3.1.2 verziószámmal kell ellátni

9.3.1.3 legalább három évig archiválni kell

9.4 Munkatársak tájékoztatása

9.4.1 A szabályzat frissítéseiről valamennyi távoli felhasználót tájékoztatni kell. Minden jelentős változást tudomásul kell vetetni.

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzat az alábbi szabályzatokhoz kapcsolódik, és azok alkalmazását támogatja:

10.1.1 P2S – Irányítási szerepkörök és felelősségek szabályzata: Meghatározza, hogy ki jogosult a távoli hozzáférés engedélyezésére és felügyeletére

10.1.2 P4S – Hozzáférés-szabályozási szabályzat: Meghatározza a biztonságos távoli hozzáférés kialakításának és visszavonásának eljárásait

10.1.3 P6S – Kockázatkezelési szabályzat: Nyomon követi és értékeli a telephelyen kívüli hozzáféréshez kapcsolódó kockázatokat

10.1.4 P8S – Információbiztonsági tudatossági és képzési szabályzat: Felkészíti a felhasználókat a távmunkával kapcsolatos kockázatokra és a bevált gyakorlatokra

10.1.5 P30S – Incidenskezelési szabályzat: Szabályozza a távoli hozzáféréssel összefüggő biztonsági incidensekre adott reagálást, például hitelesítő adatok kiszivárgása vagy eszközvesztés esetén

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 6.1. pont – Kockázatalapú tervezés távoli hozzáférési forgatókönyvek esetén

11.1.2 6.2. pont – Kezeli a humánerőforrás-felelősségi köröket mobil és távoli munkavégzési környezetben

11.1.3 8.1. pont – A távoli folyamatok operatív tervezése és szabályozása

11.2 ISO/IEC 27002

11.2.1 6.7. kontroll – Gyakorlati iránymutatást ad a távoli és mobil munkavégzés biztonságára vonatkozóan

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-17 – Távoli hozzáférés szabályozása, munkamenet-védelmi intézkedések és biztonsági felügyelet

11.3.2 AC-2 – Fiókkezelés telephelyen kívüli felhasználók esetén

11.4 EU GDPR

11.4.1 32. cikk – Előírja a megfelelő technikai és szervezési intézkedések alkalmazását, beleértve a távoli munkavégzési környezetet is

11.5 EU NIS2 irányelv

11.5.1 21. cikk (2) bekezdés b) – Előírja a hálózati és információs rendszerek biztonságos használatát

11.5.2 21. cikk (2) bekezdés h) – Humánerőforráshoz kapcsolódó biztonsági intézkedéseket ír elő, beleértve a telephelyen kívüli kontrollokat is

11.6 EU DORA

11.6.1 9. cikk – Előírja, hogy a pénzügyi szervezetek valamennyi működési módban, ideértve a távoli hozzáférést is, fenntartsák az IKT-rezilienciát

11.7 COBIT 2019

11.7.1 DSS05 – Biztonsági szolgáltatások kezelése: magában foglalja a végpontvédelem és a biztonságos távmunkavégzési gyakorlatok követelményeit

11.7.2 APO13 – Irányított biztonság: biztosítja a mobil és távoli hozzáférések biztonságos jogosultságkiosztását és kockázati felügyeletét