					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P09					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**

1. Cél

1.1 Jelen szabályzat meghatározza a távmunka biztonságos végzésére vonatkozó kötelező követelményeket, ideértve a szervezeti rendszerek használatát, az adatokhoz való hozzáférést, valamint a munkaköri feladatok vállalati telephelyen kívüli ellátását.

1.2 Biztosítja a távolról elért információs vagyon bizalmasságát, sértetlenségét és rendelkezésre állását, továbbá meghatározza az elosztott munkakörnyezetekhez kapcsolódó kockázatok csökkentését szolgáló kontrollokat.

1.3 A szabályzat az ISO/IEC 27001:2022 A mellékletének 6.7. kontrolljában foglalt követelmények teljesítését szolgálja a távmunka feltételeire szabott technikai és eljárási védelmi intézkedések bevezetésével.

2. Hatály

2.1 Jelen szabályzat minden olyan munkatársra kiterjed, aki távmunka végzésére jogosult, ideértve az alábbiakat:

2.1.1 munkavállalók (teljes munkaidős, részmunkaidős, szerződéses)

2.1.2 külső szolgáltatók, tanácsadók és beszállítók

2.1.3 ideiglenes és projektalapú munkatársak jóváhagyott távoli hozzáféréssel

2.2 A szabályzat az alábbiakra terjed ki:

2.2.1 hozzáférés a szervezeti rendszerekhez VPN-en vagy jóváhagyott távoli hozzáférési megoldásokon keresztül

2.2.2 érzékeny és szabályozott adatok kezelése védett létesítményeken kívül

2.2.3 szervezeti tulajdonú vagy BYOD (saját eszköz használata) eszközök használata

2.2.4 fizikai és logikai védelmi intézkedések távoli munkakörnyezetekben

2.3 A szabályzat minden olyan földrajzi helyszínen és időzónában alkalmazandó, ahol a szervezet a rendszeres, eseti vagy üzletmenet-folytonossági eseményhez kapcsolódó távmunka végzését engedélyezi.

3. Célkitűzések

3.1 Annak biztosítása, hogy a belső rendszerekhez és információkhoz távolról kizárólag jogosult személyek férjenek hozzá.

3.2 A titkosítás, a többtényezős hitelesítés és a végpontvédelem érvényesítése valamennyi távoli hozzáférési csatornán.

3.3 A megfelelő biztonsági helyzet fenntartása az olyan fenyegetésekkel szemben, mint az adathalászat, a kártékony kód, az adatok illetéktelen kivezetése és a rendszerek jogosulatlan elérhetővé válása.

3.4 Az érzékeny adatok telephelyen kívüli továbbítására, tárolására és nyomtatására vonatkozó szabályok meghatározása.

3.5 Olyan fizikai biztonsági intézkedések bevezetése, amelyek csökkentik a láthatóságot és a jogosulatlan megfigyelés kockázatát a távoli munkavégzés során.

3.6 A távoli adathozzáférésre vonatkozó nemzetközi jogszabályi követelményeknek való megfelelés biztosítása, beleértve a GDPR-t, a NIS2 irányelvet és a DORA-rendeletet.

4. Szerepkörök és felelősségi körök

4.1 Felső vezetés

4.1.1 Jóváhagyja ezt a szabályzatot, és biztosítja a végrehajtásához szükséges erőforrásokat, valamint annak integrálását a HR-, IT- és biztonsági működésbe.

4.1.2 Jóváhagyja a szervezeti távmunka-jogosultsági feltételeket és az üzleti egységekre vonatkozó alkalmazhatóságot.

4.2 Információbiztonsági vezető / IBIR-vezető

4.2.1 A szabályzat gazdája, gondoskodik annak karbantartásáról, valamint a kockázati helyzettel és a szabályozási követelményekkel való összhangjáról.

4.2.2 Meghatározza a távoli hozzáférés biztonsági kontrolljait (pl. titkosítás, végpontvédelem, munkamenet-időtúllépés).

4.2.3 Jóváhagyja a kivételkezelést, és nyomon követi a kontrollok hatékonyságát.

[... 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 A felülvizsgálat gyakorisága

9.1.1 Jelen szabályzatot évente, vagy szükség esetén ennél gyakrabban felül kell vizsgálni az alábbi esetekben:

9.1.1.1 új távoli hozzáférési technológiák bevezetése

9.1.1.2 a távmunka jelentős bővítése (pl. hibrid munkavégzési kezdeményezések)

9.1.1.3 új, távoli környezetekhez kapcsolódó fenyegetések, sérülékenységek vagy incidensek megjelenése

9.1.1.4 a vonatkozó jogi vagy szabályozási keretrendszerek változása

9.2 Tulajdonosi és felülvizsgálati folyamat

9.2.1 A szabályzat gazdája az információbiztonsági vezető. A felülvizsgálatot az alábbi területekkel összehangoltan kell lefolytatni:

9.2.1.1 IT-üzemeltetés és architektúra

9.2.1.2 HR és létesítménygazdálkodás (az operatív és munkakörnyezeti hatások miatt)

9.2.1.3 adatvédelmi tisztviselő (az adatvédelmi és határokon átnyúló adatkezelési kontrollok miatt)

9.2.2 A szabályzatfrissítéseket:

9.2.2.1 az IBIR irányító bizottságnak jóvá kell hagynia

9.2.2.2 valamennyi érintett munkatárssal és szerződéses közreműködővel közölni kell

9.2.2.3 be kell építeni a beléptetési és ismétlő képzési anyagokba

9.3 Dokumentumkezelés és terjesztés

9.3.1 A szabályzatnak tartalmaznia kell a verziókezelést, a hatálybalépés dátumát és a változáselőzményeket.

9.3.2 A hatályon kívül helyezett verziókat a Dokumentumkezelési szabályzat (P14) szerint meg kell őrizni.

9.3.3 A módosított verziók esetén a távmunka-végzésre jogosult felhasználók részéről kötelező ismételt tudomásulvételt kell előírni.

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzat az alábbi szabályzatokkal együtt alkalmazandó:

10.1.1 P1 – Információbiztonsági szabályzat: Meghatározza a vagyonelemek biztonságos kezelésének alapelveit, amelyek minden munkakörnyezetre, így a távmunkára is alkalmazandók.

10.1.2 P3 – Elfogadható használati szabályzat: Szabályozza a szervezeti eszközök és rendszerek megfelelő használatát a távoli munkamenetek során.

10.1.3 P4 – Hozzáférés-szabályozási szabályzat: Biztosítja, hogy a távoli hozzáférési jogosultságok a legkisebb jogosultság elve és a megfelelő hitelesítési mechanizmusok szerint kerüljenek kiosztásra.

10.1.4 P6 – Kockázatkezelési szabályzat: Meghatározza, hogyan kell a távmunka kockázatait azonosítani, kezelni és nyomon követni az IBIR keretében.

10.1.5 P12 – Eszközkezelési szabályzat: Előírja a távolról használt valamennyi eszköz nyilvántartását és konfigurációkezelését.

10.1.6 P22 – Naplózási és felügyeleti szabályzat: Biztosítja, hogy a távoli munkamenetek felügyelete, auditálása és megőrzése a megfelelőségi követelmények szerint történjen.

10.1.7 P14 – Adatmegőrzési és selejtezési szabályzat: Meghatározza a távmunkához kapcsolódó adatkezelési szabályokat, beleértve a cserélhető adathordozókat és az eszközök selejtezését.

10.2 Ezek a szabályzatok együttesen biztosítják, hogy a távmunka minden funkcióban és földrajzi helyszínen biztonságos, megfelelő és kikényszeríthető legyen.

11. Hivatkozott szabványok és keretrendszerek

11.1 Jelen szabályzat összhangban áll a nemzetközileg elismert biztonsági, adatvédelmi és IKT-kockázatkezelési keretrendszerekkel annak érdekében, hogy a távmunka gyakorlata biztonságos, visszakövethető és megfelelő legyen.

11.2 ISO/IEC 27001

11.2.1 6.1.3 pont – Kockázatkezelési tervezés: Jelen szabályzat hozzájárul a távoli hozzáféréshez és az elosztott munkakörnyezetekhez kapcsolódó kockázatok kezeléséhez.

11.2.2 8.1 pont – Operatív tervezés és szabályozás: Előírja a szervezeti telephelyen kívül elért rendszerekre vonatkozó kontrollok bevezetését.

11.2.3 A melléklet 6.7. kontrollja – Távmunka: Jelen szabályzat teljes körűen lefedi azokat a szükséges kontrollokat, amelyek az információbiztonság biztosításához szükségesek, amikor a munkatársak a szervezeti telephelyen kívül dolgoznak, beleértve a fizikai és logikai védelmi intézkedéseket, a hozzáférés-szabályozást és a felhasználói viselkedés nyomon követését.

11.3 ISO/IEC 27002:2022 – 6. kontroll

11.3.1 Ez a kontroll eljárási és technikai védelmi intézkedéseket ír elő a távmunkára. Magában foglalja az eszközbiztonságra, a hozzáférési módszerekre, az adatkezelésre, a környezeti védelmi intézkedésekre és a harmadik felek résztvevőinek kezelésére vonatkozó követelményeket, amelyeket jelen szabályzat érvényesít.

11.4 NIST SP 800-53 Rev.5

11.4.1 AC-17 (Távoli hozzáférés): Közvetlenül támogatott VPN-kontrollokkal, többtényezős hitelesítéssel, munkamenet-naplózással és szerepköralapú hozzáférés-jóváhagyással a távoli felhasználók számára.

11.4.2 AC-2 (Fiókkezelés): Szabályozza a hozzáférési jogosultságot, a távoli jogosultságok hozzárendelését és a fiókok letiltását.

11.4.3 SC-12–SC-13 (Kriptográfiai védelem, kriptográfiai kulcsok létrehozása): A távoli végpontok esetében kötelező VPN-használattal és teljes lemeztitkosítással valósul meg.

11.4.4 MP-5 (Adathordozók szállításának védelme) és PE-18 (Az információs rendszer összetevőinek elhelyezkedése): A távmunka-előírások külső helyszíneken előírják a szállítás közbeni védelmet és a fizikai védelmi intézkedéseket.

11.4.5 AU-2, AU-6: A távoli munkamenetek naplózása és felügyelete támogatja az audit- és incidenskezelési követelményeket.

11.5 GDPR (2016/679)

11.5.1 32. cikk – Az adatkezelés biztonsága: Jelen szabályzat érvényesíti a személyes adatok távoli elérése vagy kezelése során szükséges távoli hozzáférési biztonsági, titkosítási és naplózási kontrollokat.

11.5.2 5. cikk (1) bekezdés f) pont: Biztosítja, hogy a telephelyen kívül elért személyes adatok védettek legyenek a jogosulatlan vagy jogellenes adatkezeléssel és a véletlen elvesztéssel szemben.

11.5.3 39. preambulumbekezdés: Hangsúlyozza a hozzáférés korlátozását, a sértetlenséget és a bizalmasságot, különösen akkor, amikor az eszközök elhagyják a védett telephelyet.

11.6 NIS2 irányelv (2022/2555)

11.6.1 21. cikk (2) bekezdés a), b), d) pont: Előírja, hogy a távoli hozzáférést a szervezet IKT-kockázatkezelési keretrendszerének részeként biztosítani kell. Jelen szabályzat teljesíti a hozzáférés-szabályozást, az adatbiztonságot és a távoli környezetekre vonatkozó szervezeti szabályzatokat lefedő biztonsági intézkedésekre vonatkozó követelményeket.

11.6.2 21. cikk (3) bekezdés: Előírja a biztonságtudatosság erősítését és a szabályzatok betartását a központi telephelyeken kívül dolgozó munkatársak körében.

11.7 DORA-rendelet (2022/2554)

11.7.1 5. cikk – Irányítási és belső kontroll keretrendszer: Jelen szabályzat támogatja az IKT-kockázati kontrollokra vonatkozó elvárásokat minden operatív helyzetben, beleértve a hibrid és távoli működési modelleket is.

11.7.2 8. cikk – IKT-kockázatkezelési keretrendszer: A távoli hozzáférés kockázatait a jelen szabályzatban meghatározott technikai és szervezeti kontrollok azonosítják, csökkentik és kezelik.

11.7.3 9. cikk – Információmegosztási megállapodások: Védelmet nyújt a digitális működési reziliencia-hálózatokon belül megosztott információk távoli kiszivárgása ellen.

11.8 COBIT 2019

11.8.1 DSS01 – Menedzselt üzemeltetés: Jelen szabályzat támogatja az üzleti működés biztonságos folytonosságát a fizikai helytől függetlenül.

11.8.2 BAI06 – Menedzselt IT-változtatások és BAI09 – Menedzselt eszközök: Biztosítják, hogy a távmunkához használt eszközök nyomon követettek, biztonságosan konfiguráltak és kritikus eszközként kezeltek legyenek.

11.8.3 APO13 – Menedzselt biztonság: Elősegíti a távoli környezetekre vonatkozó meghatározott biztonsági irányítási keretrendszert.

11.8.4 MEA03 – Megfelelés nyomon követése, értékelése és felmérése: Meghatározza, hogy a távmunka-tevékenységet naplózni, felülvizsgálni és auditálni kell.