					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P11S					Dokumentum címe: **Felhasználói fiók- és jogosultságkezelési 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	5.3., 8. pont	Szerepkörök, felelősségi körök, valamint operatív tervezés és kontroll a felhasználói hozzáférések kezeléséhez
ISO/IEC 27002:2022	8. kontroll	Kontrollok az emelt jogosultságok kiosztására, felülvizsgálatára és eltávolítására
NIST SP 800-53 Rev.5	AC-2, AC-5, AC-6	Fióklétrehozás, nyomon követés, a legkisebb jogosultság elve és a feladatkörök szétválasztása
EU NIS2	21. cikk (2) bekezdés d) pont	Felhasználói hozzáférések kezelése az alapvető és fontos szervezeteknél
EU DORA	9. cikk (2) bekezdés b) pont	Emelt jogosultságok hozzáférés-szabályozása pénzügyi szervezeteknél
COBIT 2019	DSS05.03, DSS05.04	Jogosultságkiosztás, hozzáférés megszüntetése és a felhasználói hozzáférések időszakos felülvizsgálata
EU GDPR	32. cikk	Megfelelő hozzáférés-szabályozás a személyes adatok védelme érdekében

1. Cél

1.1 Jelen szabályzat meghatározza a felhasználói fiókok és hozzáférési jogosultságok biztonságos, egységes és visszakövethető kezelésének szabályait. Biztosítja, hogy rendszerekhez és adatokhoz kizárólag jogosult felhasználók férjenek hozzá, és a hozzáférés mértéke igazodjon szerepkörükhöz és felelősségi körükhöz.

1.2 A hatékony fiók- és jogosultságkezelés alapvető fontosságú a jogosulatlan hozzáférés megelőzése, a belső fenyegetések mérséklése, valamint az ISO/IEC 27001, a GDPR és egyéb szabályozási követelmények teljesítése szempontjából.

1.3 Ez a szabályzat lehetővé teszi a szervezet számára, hogy kijelölje a fiókhasználathoz kapcsolódó tulajdonosi és felelősségi köröket, nyomon kövesse és auditálja a jogosultságemeléseket, valamint biztonságosan letiltsa vagy visszavonja a hozzáférést, amikor arra már nincs szükség.

1.4 A szabályzat emellett védi az üzleti működést a túlzott vagy nem felügyelt hozzáférésekből eredő működési hibáktól és visszaélésektől, valamint csökkenti a véletlen adatvesztés, a jogosultságokkal való visszaélés és a szabályozói meg nem felelés kockázatát.

2. Hatály

2.1 Jelen szabályzat az alábbiakra terjed ki:

2.1.1 valamennyi munkavállalóra, gyakornokra, szerződéses közreműködőre és harmadik fél felhasználóra, akik hozzáférnek a szervezet IT-rendszereihez

2.1.2 valamennyi olyan rendszerre, eszközre, szolgáltatásra és platformra, amelyet a szervezet vagy a szervezet nevében kezelnek, ideértve a felhőplatformokat, a helyszíni infrastruktúrát és a harmadik fél által biztosított eszközöket

2.2 A szabályzat a felhasználói fiókok minden típusára kiterjed, ideértve az alábbiakat:

2.2.1 névre szóló felhasználói fiókok (pl. e-mail-fiókok, rendszerbejelentkezések)

2.2.2 adminisztrátori és rendszerszintű fiókok

2.2.3 ideiglenes, vendég- vagy harmadik fél részére biztosított hozzáférési hitelesítő adatok

2.2.4 alkalmazások vagy automatizált rendszerek által használt szolgáltatásfiókok

2.3 A szabályzat a fiókok teljes életciklusára alkalmazandó, a létrehozástól és jóváhagyástól kezdve a módosításon és nyomon követésen át a deaktiválásig. Ez magában foglalja a kezdeti jogosultságkiosztást a beléptetés során, a hozzáférés-felülvizsgálatokat szerepkör-változás esetén, valamint a hozzáférés megszüntetését a kiléptetés során.

3. Célkitűzések

3.1 Minden rendszerfelhasználóhoz egyedi, visszakövethető felhasználói azonosítót kell rendelni, biztosítva az elszámoltathatóságot és kizárva a megosztott hitelesítő adatok használatát.

3.2 Érvényesíteni kell a legkisebb jogosultság elvét annak biztosítása érdekében, hogy a felhasználók kizárólag a feladataik ellátásához minimálisan szükséges hozzáférést kapják meg.

3.3 A bizalmas rendszerekhez vagy adatokhoz való jogosulatlan hozzáférést egyértelműen dokumentált jóváhagyási és felülvizsgálati folyamatokkal kell megelőzni.

3.4 Biztosítani kell a felhasználói fiókok időben történő deaktiválását, amennyiben azokra már nincs szükség, például munkaviszony megszűnése, szerződés lezárása vagy szerepkör-változás esetén.

3.5 A fiókmódosítások, jóváhagyások és időszakos felülvizsgálatok dokumentálásával fenn kell tartani a biztonságos, az auditra való felkészültséget támogató környezetet.

3.6 Biztosítani kell, hogy a jogosultságemelés szigorúan szabályozott, függetlenül jóváhagyott és naplózott legyen, továbbá az emelt hozzáférést haladéktalanul vissza kell vonni, amikor arra már nincs szükség.

4. Szerepkörök és felelősségi körök

4.1 Ügyvezető

4.1.1 Átfogó elszámoltathatósággal tartozik jelen szabályzat betartatásáért.

4.1.2 Biztosítja, hogy a fiókkezelési gyakorlat összhangban álljon az ISO/IEC 27001 tanúsítási követelményeivel és a vonatkozó jogi kötelezettségekkel (pl. GDPR).

4.1.3 Haladéktalanul tájékoztatni kell minden olyan jogosulatlan hozzáférésről, biztonsági incidensről vagy szabályzatsértésről, amely felhasználói fiókokhoz kapcsolódik.

4.1.4 Felügyeli a szabályzat felülvizsgálatait, auditjait és a kapcsolódó végrehajtási intézkedéseket.

4.2 Informatikai vezető vagy külső IT-szolgáltató

4.2.1 Felelős a fiók- és jogosultságkezelési kontrollok technikai bevezetéséért a szervezet által használt rendszerekben.

4.2.2 Kizárólag dokumentált jóváhagyás alapján hozhat létre, módosíthat vagy szüntethet meg felhasználói fiókokat.

4.2.3 Köteles érvényesíteni a jelszókomplexitási követelményeket, a képernyőzár időkorlátját, a többtényezős hitelesítést (ha rendelkezésre áll), valamint a rendszernaplózást.

4.2.4 Köteles biztonságosan megőrizni az összes hozzáférési jóváhagyásra, fióktulajdonosi felelősségre, jogosultságemelésre és visszavonásra vonatkozó nyilvántartást.

4.2.5 Köteles figyelemmel kísérni a jogosulatlan vagy árva fiókok jelenlétét, és az eltéréseket jelenteni az ügyvezetőnek.

[... 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 Jelen szabályzatot az ügyvezetőnek és az informatikai vezetőnek legalább évente felül kell vizsgálnia az alábbiakkal való összhang biztosítása érdekében:

9.1.1 az aktuális ISO/IEC 27001:2022 kontrollokkal és iránymutatásokkal

9.1.2 a szabályozási változásokkal (pl. GDPR, DORA, NIS2)

9.1.3 a rendszerekben, szolgáltatásokban vagy az üzleti struktúrában bekövetkezett változásokkal

9.2 Felülvizsgálatot kell végezni az alábbi eseteket követően is:

9.2.1 jelentős biztonsági incidensek vagy auditmegállapítások

9.2.2 az IT-rendszerekben vagy a fiókarchitektúrában végrehajtott jelentős változások

9.2.3 új, hozzáférés-szabályozási integrációt igénylő platformok bevezetése

9.3 Minden módosítást az ügyvezetőnek jóvá kell hagynia, és azokat egyértelműen kommunikálni kell az érintett munkatársak felé.

10. Kapcsolódó szabályzatok és összefüggések

10.1 P2S – Irányítási szerepkörök és felelősségek szabályzata: meghatározza a hozzáférési jóváhagyásokhoz és a felügyelethez kapcsolódó elszámoltathatóságot és döntési jogosultságot.

10.2 P4S – Hozzáférés-szabályozási szabályzat: szabályozza a rendszerszintű hozzáférés-szabályozás érvényesítését és a hitelesítési módszereket.

10.3 P7S – Beléptetési és kiléptetési szabályzat: biztosítja, hogy a fióklétrehozás és a hozzáférés megszüntetése beépüljön a HR által kezelt személyi változásokba.

10.4 P8S – Információbiztonsági tudatossági és képzési szabályzat: oktatja a felhasználókat a biztonságos fiókhasználatra és a használati elvárásokra.

10.5 P30S – Incidenskezelési szabályzat: meghatározza a szükséges intézkedéseket arra az esetre, ha a fiókokkal való visszaélés biztonsági incidenshez vagy jogosulatlan közzétételhez vezet.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 5.3. pont: előírja, hogy az információbiztonsághoz kapcsolódó szerepköröket és felelősségi köröket egyértelműen ki kell jelölni, és azok betartását biztosítani kell.

11.1.2 8.1. pont: előírja, hogy az operatív tervezésnek és kontrollnak ki kell terjednie a felhasználói hozzáférések kezelésére.

11.2 ISO/IEC 27002

11.2.1 8.2. kontroll: részletezi az emelt jogosultságok kiosztására, felülvizsgálatára és eltávolítására szolgáló technikai és eljárási kontrollokat.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-2: előírja a fiókok létrehozását, nyomon követését és visszavonását meghatározott szerepkörök és folyamatok alapján.

11.3.2 AC-5: előírja a feladatkörök szétválasztását a jogosultsági összeférhetetlenség vagy visszaélés megelőzése érdekében.

11.3.3 AC-6: előírja a legkisebb jogosultság elvének alkalmazását valamennyi hozzáférési jogosultságra.

11.4 EU GDPR

11.4.1 32. cikk: megfelelő hozzáférés-szabályozást ír elő a személyes adatok jogosulatlan hozzáféréssel vagy módosítással szembeni védelme érdekében.

11.5 EU NIS2

11.5.1 21. cikk (2) bekezdés d) pont: előírja a felhasználói hozzáférések kezelését mint az alapvető és fontos szervezetekre vonatkozó alapvető biztonsági kontroll részét.

11.6 EU DORA

11.6.1 9. cikk (2) bekezdés b) pont: előírja, hogy a pénzügyi szervezetek olyan hozzáférés-szabályozást vezessenek be, amely korlátozza és felügyeli az emelt jogosultságokat.

11.7 COBIT 2019

11.7.1 DSS05.03: az IT-irányítás részeként meghatározza a felhasználói hozzáférések jogosultságkiosztását és a hozzáférés megszüntetését.

11.7.2 DSS05.04: előírja a felhasználói hozzáférések folyamatos felülvizsgálatát és a szervezeti szerepkörökkel való összhang biztosítását.