					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P11					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	6.1.3. pont, 8. fejezet	-
ISO/IEC 27002:2022	5.15–5.18 kontrollok	-
GDPR	5. cikk (1) bekezdés f) pont, 32. cikk, (39) preambulumbekezdés	-
NIS2 irányelv	21. cikk (2) bekezdés a), d) pont, 21. cikk (3) bekezdés	-
DORA-rendelet	5. cikk, 9. cikk	-
COBIT 2019	DSS01, DSS05, APO13	-

1. Cél

1 Ez a szabályzat kötelező kontrollokat határoz meg a felhasználói fiókok és jogosultságok kezelésére valamennyi információs rendszerben és szolgáltatásban. Biztosítja, hogy a szervezeti erőforrásokhoz való hozzáférés kizárólag ellenőrzött identitás, munkaköri indokoltság, valamint a legkisebb jogosultság elve és a feladatkörök szétválasztása alapján kerüljön megadásra.

1.1 A szabályzat támogatja a szervezet információbiztonság iránti elkötelezettségét azáltal, hogy strukturált, auditálható folyamatokat vezet be a jogosultságok engedélyezése, hozzárendelése, használatának nyomon követése és a hozzáférés megszüntetése terén.

1.2 Ez a szabályzat kiemelt jelentőségű a jogosulatlan hozzáférés, a jogosultságokkal való visszaélés, a belső fenyegetések és az alkalmazandó szabályozási keretrendszerek szerinti meg nem felelés kockázatának csökkentése szempontjából.

2. Hatály

2.1 Ez a szabályzat valamennyi munkavállalóra, szerződéses közreműködőre, harmadik fél szolgáltatóra, tanácsadóra és minden más olyan személyre alkalmazandó, aki hozzáférést kap a szervezet IT-erőforrásaihoz, alkalmazásaihoz vagy adataihoz.

2.2 A szabályzat minden olyan rendszerre és környezetre kiterjed, ahol felhasználói hitelesítés és hozzáférés-szabályozás működik, beleértve többek között az alábbiakat:

2.2.1 Vállalati alkalmazások és adatbázisok

2.2.2 Felhőplatformok és SaaS-környezetek

2.2.3 Operációs rendszerek és adminisztrációs konzolok

2.2.4 Távoli hozzáférési eszközök és VPN-ek

2.2.5 Identitás- és hozzáférés-kezelési (IAM) rendszerek

2.3 A szabályzat kiterjed a standard és az emelt jogosultságú fiókokra egyaránt, és az alábbi területek feletti kontrollokat is magában foglalja:

2.3.1 Fiókok létrehozása, módosítása és deaktiválása

2.3.2 Jogosultságeszkaláció és delegálás

2.3.3 Munkamenet-kezelés és nyomon követés

2.3.4 Hitelesítési módszerek és hitelesítő adatok kezelése

3. Célkitűzések

3.1 Annak biztosítása, hogy minden felhasználói fiók egyedileg azonosítható és megfelelően engedélyezett legyen, továbbá kizárólag a szükségesség formális ellenőrzését követően kerüljön hozzárendelésre.

3.2 A legkisebb jogosultság elvének alkalmazása, valamint a szükségtelen vagy túlzott hozzáférések megelőzése az emelt jogosultságú fiókok kiadására és használatára vonatkozó szigorú kontrollok érvényesítésével.

3.3 A fiókállapot időben történő frissítésének előírása a munkaviszonyban vagy szerepkörben bekövetkező változások alapján, beleértve a hozzáférés azonnali megszüntetését a munkaviszony megszűnésekor.

3.4 Az inaktív, nem megfelelően használt vagy jogosulatlan fiókok proaktív észlelésének és a helyesbítő intézkedések megtételének biztosítása naplózás, felülvizsgálatok és automatizálás útján.

3.5 Az ISO/IEC 27001:2022 és a kapcsolódó szabványokkal való összhang fenntartása, továbbá a GDPR, a NIS2, a DORA és a COBIT 2019 szerinti vonatkozó jogi és szabályozási kötelezettségek teljesítése.

4. Szerepkörök és felelősségi körök

4.1 Információbiztonsági vezető

4.1.1 A szabályzat gazdája, és biztosítja annak végrehajtását a szervezet egészében.

4.1.2 Felülvizsgálja és jóváhagyja a formális kivételeket, valamint a sürgősségi hozzáférési eseteket.

4.1.3 Jelenti a fiókkezeléssel kapcsolatos auditmegállapításokat, és a kockázatokat a felső vezetés felé eszkalálja.

4.2 Hozzáférés-kezelési vezető / IT-rendszergazda

4.2.1 Fenntartja és üzemelteti a felhasználói fiókok életciklus-kezeléséhez kapcsolódó technikai kontrollokat.

4.2.2 Jóváhagyott kérelem alapján végrehajtja a jogosultságok kiosztását, a hozzáférés megszüntetését és a jogosultságkezelési intézkedéseket.

4.2.3 Vezeti valamennyi felhasználói fiók, azok állapota és jogosultsági szintje hiteles nyilvántartását.

4.2.4 Támogatja az auditokat és a megfelelőségi felülvizsgálatokat naplókkal és tevékenységi jelentésekkel.

[... 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 jelen szabályzatot legalább évente, illetve az alábbi területeket érintő jelentős változás esetén felül kell vizsgálni:

9.1.1 a szervezeti struktúrát vagy üzleti folyamatokat,

9.1.2 az IT-rendszereket, identitásplatformokat vagy hozzáférési módszereket,

9.1.3 az identitás- és hozzáférés-kezeléshez kapcsolódó szabályozási vagy szerződéses követelményeket.

9.2 Az információbiztonsági vezető a hozzáférés-kezelési vezetővel együtt felelős a felülvizsgálati folyamat megindításáért és az érintettek visszajelzéseinek összehangolásáért.

9.3 Soron kívüli felülvizsgálatot válthat ki különösen:

9.3.1 a fiókokkal való visszaéléshez kapcsolódó biztonsági incidens,

9.3.2 a fiókéletciklus-kezelés hiányosságait feltáró auditmegállapítás,

9.3.3 új identitáskezelési vagy emelt jogosultságú hozzáférés-kezelési eszköz bevezetése.

9.4 A szabályzat módosításait:

9.4.1 verziókezelés alá kell vonni, és az IBIR dokumentációs tárában rögzíteni kell,

9.4.2 közölni kell valamennyi releváns érintettel, beleértve a szervezeti egység vezetőket, az IT-üzemeltetést és a HR-t,

9.4.3 aktualizált képzési anyagokkal és eljárásrendekkel kell alátámasztani.

9.5 Valamennyi módosítást a felső vezetésnek vagy az információbiztonsági irányító bizottságnak kell jóváhagynia, és auditcélból naplózni kell.

10. Kapcsolódó szabályzatok és összefüggések

10.1 Ez a szabályzat működési szempontból az alábbi, az IBIR keretében alkalmazott kapcsolódó szabályzatokhoz kapcsolódik, és azokat támogatja:

10.1.1 P4 Hozzáférés-szabályozási szabályzat: Meghatározza a hozzáférés-szabályozás átfogó elveit és mechanizmusait, beleértve a szabályalapú és szerepköralapú kontrollokat.

10.1.2 P7 Beléptetési és kiléptetési szabályzat: Eljárási lépéseket rögzít a felhasználói hozzáférés HR-intézkedésekhez igazodó kezdeményezéséhez és megszüntetéséhez.

10.1.3 P8 Információbiztonsági tudatossági és képzési szabályzat: Megerősíti a felhasználói felelősségeket a fiókbiztonság és a hitelesítő adatok védelme terén.

10.1.4 P13 Adatosztályozási és címkézési szabályzat: Az adatosztályozás alapján iránymutatást ad a hozzáférési szintekhez, biztosítva, hogy a jogosultsági határok összhangban legyenek az érzékenységi szintekkel.

10.1.5 P22 Naplózási és felügyeleti szabályzat: Biztosítja, hogy minden fiókkezeléssel kapcsolatos tevékenységről auditnyom álljon rendelkezésre, és azt rendellenességek vagy jogosulatlan használat észlelése céljából felülvizsgálják.

10.1.6 P30 Incidenskezelési szabályzat: Szabályozza az eszkalációt, az elszigetelést és az incidens utáni intézkedéseket a jogosultságokkal való visszaélés vagy a jogosulatlan fióktevékenység eseteiben.

10.2 E szabályzatok együttesen biztosítják a szervezeten belüli egységes, kockázatalapú identitáskezelési és hozzáférés-szabályozási keretrendszer érvényesítését.

11. Hivatkozott szabványok és keretrendszerek

11.1 Ez a szabályzat összhangban áll a nemzetközileg elismert kiberbiztonsági szabványokkal és szabályozási keretrendszerekkel, amelyek a biztonságos identitáskezelést, hozzáférés-szabályozást és jogosultságkezelést a szervezeti információbiztonság alapvető elemévé teszik.

11.2 ISO/IEC 27001:

11.2.1 A 6.1.3. pont előírja, hogy a szervezetnek meg kell határoznia, értékelnie kell és kezelnie kell az információbiztonsági kockázatokat, ezáltal a hozzáférés- és jogosultságkezelés az IBIR tervezési folyamatába beépített, formális, kockázatalapú kontrollként jelenik meg.

11.2.2 A 8.1. pont – Működéstervezés és szabályozás – megerősíti azon technikai és eljárási védelmi intézkedések bevezetését, amelyek a felhasználói és emelt jogosultságú hozzáférést szabályozzák.

11.3 ISO/IEC 27002:2022 – 5.15–5.18 kontrollok:

11.3.1 5.15. kontroll – Felhasználói hozzáférés-kezelés: Támogatja a fiókok jogosultságkiosztására, a hozzáférés engedélyezésére és a hozzáférési jogosultságok időszakos felülvizsgálatára vonatkozó formális folyamatokat.

11.3.2 5.16. kontroll – Identitáskezelés: Meghatározza az identitások egyediségét, az életciklus-kontrollokat és a biztonságos hitelesítés érvényesítését.

11.3.3 5.17. kontroll: Biztosítja, hogy a hitelesítési információk kiosztása és kezelése szigorúan szabályozott, visszakövethető és a felhasználói fiók teljes életciklusa során ellenőrzött legyen.

11.3.4 5.18. kontroll – Hozzáférési jogosultságok: A jelen szabályzat teljes körűen kezeli szerepköralapú jogosultság-hozzárendeléssel, auditálással és az emelt jogosultságú hozzáférések jóváhagyási követelményeivel.

11.4 Ezek a kontrollok iránymutatást adnak a fiókregisztráció, a törlés, a jogosultságok elkülönítése és a hitelesítési információk használata strukturált bevezetéséhez. A szabályzat érvényesíti az identitás-életciklus irányítását, a just-in-time hozzáférést és az emelt jogosultságú munkamenetek nyomon követését a jogosulatlan rendszerhasználat megelőzése érdekében.

11.5 NIST SP 800-53 Rev.5:

11.5.1 AC-1 (Hozzáférés-szabályozási szabályzat) és AC-2 (Fiókkezelés): A szabályzat hozzáférés-jóváhagyásra, szerepkör-hozzárendelésre és felhasználói fiókok auditálására vonatkozó előírásai révén kerülnek leképezésre.

11.5.2 AC-5 (Feladatkörök szétválasztása) és AC-6 (Legkisebb jogosultság elve): A jogosultságok korlátozásán, a munkaköri szerepkörökhöz igazításon és a magas kockázatú feladatok kettős jóváhagyásán keresztül teljesülnek.

11.5.3 IA-2–IA-5 (Azonosítás és hitelesítés): Erős hitelesítési mechanizmusok, a hitelesítő adatok életciklusára vonatkozó szabályok és a többtényezős hitelesítés követelményei útján érvényesülnek.

11.5.4 AU-2, AU-12 (Auditnaplózás és elemzés): Az érzékeny környezetekben megvalósított munkamenet-rögzítésen és az emelt jogosultságú tevékenységek nyomon követésén keresztül kerülnek kezelésre.

11.6 GDPR (2016/679):

11.6.1 32. cikk – Az adatkezelés biztonsága: Előírja a személyes adatok védelmét biztosító hozzáférés-szabályozási és identitás-ellenőrzési mechanizmusokat. Ennek a szabályzat a fiókengedélyezések, jogosultság-felülvizsgálatok és erős hitelesítési védelmi intézkedések kötelezővé tételével felel meg.

11.6.2 5. cikk (1) bekezdés f) pont – Sértetlenség és bizalmasság: Biztosítja, hogy személyes adatokhoz kizárólag jogosult, megfelelő szerepkörrel rendelkező felhasználók férhessenek hozzá, amelyet a fiókkezelési kontrollok érvényesítése erősít meg.

11.6.3 (39) preambulumbekezdés: Egyértelmű hozzáférés-korlátozást és elszámoltathatóságot követel meg; a jelen szabályzat ezt a felhasználói identitások és jogosultság-hozzárendelések teljes visszakövethetőségével támogatja.

11.7 NIS2 irányelv (2022/2555):

11.7.1 21. cikk (2) bekezdés a), d) pont: Előírja a hozzáférés-kezelési szabályzatok alkalmazását, valamint a hitelesítő adatok és emelt jogosultságú munkamenetek biztonságos kezelését, amelyet a jelen szabályzat jogosultságkiosztási, nyomon követési és kivételkezelési kontrolljai támogatnak.

11.7.2 21. cikk (3) bekezdés: Támogatja a hozzáférési fegyelem és az erős identitásbizonyosság érvényesítését kritikus ágazatokban, amely az egyedi azonosítók, a szerepköralapú hozzáférés-szabályozás és az időkorlátos emelt hozzáférések használatával teljesül.

11.8 DORA-rendelet (2022/2554):

11.8.1 5. cikk – IKT-irányítás és kontroll: Előírja az IKT-felhasználók kezelésére vonatkozó formalizált folyamatokat, amelyeket a dokumentált jogosultságkiosztás, deaktiválás és kivételkezelés fed le.

11.8.2 9. cikk – IKT-kockázatkezelés: Előírja, hogy a szervezetek hozzáférés-korlátozásokkal és nyomon követéssel védjék rendszereiket, amit a többtényezős hitelesítés, az emelt jogosultságú hozzáférések naplózása és a központosított felülvizsgálatok biztosítanak.

11.9 COBIT 2019:

11.9.1 DSS01 – Felügyelt üzemeltetés: Előmozdítja a szabványosított operatív kontrollok alkalmazását, beleértve a felhasználói fiókok életciklus-kezelését és a hozzáférési dokumentációt.

11.9.2 DSS05 – Biztonsági szolgáltatások kezelése: Tükrözi a felhasználói és rendszerszintű jogosultságok biztonságos adminisztrációját, támogatva a kockázatcsökkentést a legkisebb jogosultság elve és az auditnyom ellenőrzése révén.

11.9.3 APO13 – Felügyelt biztonság: Előírja a digitális vagyonelemekhez kapcsolódó hozzáférés-szabályozást, amelyet a formális fiók- és szerepkörengedélyezési gyakorlatok, valamint az időszakos felülvizsgálati kötelezettségek teljesítenek.