					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P04					Dokumentum címe: **Hozzáférés-szabályozási 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**

Jogi nyilatkozat (szerzői jog és felhasználási korlátozások)

(C) 2025 Clarysec LLC. All rights reserved.

Ez a dokumentum a Clarysec LLC szellemi tulajdona. A dokumentum semmilyen része nem másolható, nem használható fel újra, nem terjeszthető és nem módosítható kereskedelmi vagy bevezetési célból előzetes, kifejezett írásbeli engedély nélkül.

A jogosulatlan felhasználás szigorúan tilos, és jogi eljárást vonhat maga után.

Licenceléssel kapcsolatban keresse: info@clarysec.com

A vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	5.15, 5.17 és 5.18 pont	Logikai és fizikai hozzáférés kezelése
ISO/IEC 27002:2022	8.2 és 8.3 kontroll	Szerepköralapú hozzáférés és identitáskezelés
NIST SP 800-53 Rev.5	AC-1–AC-20, IA-1–IA-8	Fiók- és hozzáférés-kezelési kontrollok, azonosítás és hitelesítés
GDPR	5. cikk (1) bekezdés f) pont, 32. cikk (1) bekezdés b) pont; (39) preambulumbekezdés	Adatvédelem és adattakarékosság
NIS2 irányelv	21. cikk (2) bekezdés c)–e) pont	Hozzáférés-szabályozás, felhasználó-hitelesítés és eszközvédelem
DORA-rendelet	6. cikk, 9. cikk (2) bekezdés	IKT- és felhasználói hozzáférés, valamint erős kontrollok / harmadik felek
COBIT 2019	APO07, BAI03, DSS01, DSS05, MEA03	Beléptetés, üzemeltetés, nyomon követés, megfelelés

1. Cél

1.1 Jelen szabályzat meghatározza a szervezeten belüli információs rendszerekhez, alkalmazásokhoz, fizikai létesítményekhez és adateszközökhöz való hozzáférés kezelésére vonatkozó kötelező alapelveket, felelősségi köröket és kontrollkövetelményeket.

1.2 Biztosítja, hogy a hozzáférés engedélyezése üzleti szükségesség, munkakör és kockázati kitettség alapján történjen, különösen a legkisebb jogosultság, a szükséges ismeret és a feladatkörök elkülönítése elveinek érvényesítésével.

1.3 A szabályzat támogatja az ISO/IEC 27001:2022 5.15 pontjának, valamint a logikai és fizikai hozzáférésre, a felhasználói hitelesítésre és a hozzáférések teljes életciklusának kezelésére vonatkozó kapcsolódó kontrollok végrehajtását.

1.4 Jelen szabályzat megalapozza a digitális és fizikai erőforrások védelmét a jogosulatlan használattal, visszaéléssel és kompromittálódással szemben.

2. Hatály

2.1 Jelen szabályzat az ISMS hatálya alá tartozó valamennyi felhasználóra, rendszerre és létesítményre kiterjed, beleértve az alábbiakat:

2.1.1 munkavállalók, szerződéses partnerek, beszállítók és ideiglenes személyzet

2.1.2 helyszíni infrastruktúra, felhőalapú rendszerek és hibrid környezetek

2.1.3 valamennyi vállalati eszköz – hardver, szoftver, adatok és védett fizikai területek

2.1.4 logikai hozzáférés (pl. rendszerek, hálózatok, alkalmazások, API-k) és fizikai hozzáférés (pl. épületek, adatközpontok)

2.2 A szabályzat a személyazonosságok és az erőforrásokhoz fűződő kapcsolatok teljes életciklusára vonatkozik, a beléptetéstől és jogosultságkiosztástól a szerepkörváltáson át a kiléptetésig.

2.3 A szabályzat kiterjed a saját eszköz használatára (BYOD) és a távoli hozzáférésre is, biztosítva, hogy a kontrollok a helyszíntől és az eszköztulajdonlási modelltől függetlenül egységesen érvényesüljenek.

3. Célkitűzések

3.1 Biztonságos, szerepköralapú hozzáférés-szabályozás bevezetése, amely támogatja a működési integritást és a szabályozói megfelelést.

3.2 Annak biztosítása, hogy a hozzáférési jogosultságok megfelelő jóváhagyással, nyomon követhető módon kerüljenek kiadásra és időben visszavonásra.

3.3 A jogosulatlan hozzáférés, a jogosultságkiterjesztés és az elavult hozzáférési jogosultságok fennmaradásának megelőzése.

3.4 A zéró bizalom elveinek támogatása azáltal, hogy a hozzáférés alapértelmezetten tiltott, kivéve, ha azt kifejezetten jóváhagyták és indokolták.

3.5 Az auditorok és az érintett felek számára megfelelő bizonyosság nyújtása bizonyítékokon alapuló, automatizált hozzáférés-felülvizsgálatok és szabályzati kontrollok alkalmazásával.

3.6 A hozzáférés-szabályozás beépítése az üzleti folyamatokba, a HR-életciklus eseményeibe és a technikai architektúrákba.

4. Szerepkörök és felelősségi körök

4.1 Felsővezetés

4.1.1 Jóváhagyja a hozzáférés-szabályozási szabályzatot, és biztosítja a végrehajtásához szükséges megfelelő költségvetést és erőforrásokat.

4.1.2 A vezetőségi átvizsgálások során áttekinti a hozzáférés-szabályozási kockázatokat, és stratégiai szinten kijelöli a felelősségi köröket.

4.2 Információbiztonsági vezető / ISMS-vezető

4.2.1 Felel a hozzáférés-szabályozási keretrendszerért, és biztosítja annak összhangját az ISO/IEC 27001 és a kapcsolódó szabványok követelményeivel.

4.2.2 Koordinálja a szabályzat alkalmazását, a kontrollok tesztelését és a hozzáférés-szabályozási mutatók jelentését.

4.2.3 Felügyeli a kockázatalapú hozzáférési modell kialakítását, és nyomon követi a rendszerszintű kontrollhiányosságokat.

[... 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 esetei és gyakorisága

9.1.1 Jelen szabályzatot felül kell vizsgálni:

9.1.1.1 évente, vagy

9.1.1.2 az IT-infrastruktúrát, a szabályozói követelményeket vagy a kockázati kitettséget érintő jelentős változást követően

9.1.1.3 olyan incidensek után, amelyek a hozzáférési kontrollok gyengeségeit tárják fel

9.1.1.4 ha jelentős változás történik a hitelesítési technológiákban vagy az identitásplatformokban

9.2 A felülvizsgálat felelőse és folyamata

9.2.1 A CISO vagy a kijelölt ISMS-felelős irányítja a felülvizsgálati ciklust, amelybe beépíti az alábbiakat:

9.2.1.1 belső auditmegállapítások

9.2.1.2 a hozzáférés-felülvizsgálatok eredményei és mutatói

9.2.1.3 jogi és szabályozói változások

9.2.1.4 a technológiai platformok változásai

9.2.2 Minden módosítást a felsővezetésnek jóvá kell hagynia, és azokról valamennyi érintettet tájékoztatni kell.

9.2.3 Jelentős módosítások esetén az érintett felhasználók kötelezhetők a szabályzat ismételt tudomásulvételére.

9.3 Verziókezelés és dokumentáció

9.3.1 A mesterpéldányt az ISMS dokumentumtárban kell tárolni az alábbi metaadatokkal:

9.3.1.1 verziószám és változásnapló

9.3.1.2 hatálybalépés dátuma és a következő felülvizsgálat dátuma

9.3.1.3 tulajdonos és jóváhagyó

9.3.1.4 terjesztési és tudomásulvételi nyilvántartások

9.3.2 A hatályon kívül helyezett verziókat archiválni kell, és azokat legalább 3 évig hozzáférhetővé kell tenni.

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzat az alábbi szabályzatokkal együtt értelmezendő, és azokhoz funkcionálisan kapcsolódik:

10.1.1 P01 – Információbiztonsági szabályzat: Meghatározza a szervezet biztonsági elkötelezettségét és a hozzáférés-szabályozás magas szintű elvárásait.

10.1.2 P03 – Elfogadható használati szabályzat: Rögzíti a hozzáféréshez kapcsolódó magatartási feltételeket és a felhasználók felelősségét a rendszerek megfelelő használatáért.

10.1.3 P05 – Változáskezelési szabályzat: Szabályozza, hogy a hozzáférési konfigurációk, szerepkörök vagy csoportstruktúrák módosításait hogyan kell biztonságosan végrehajtani és tesztelni.

10.1.4 P07 – Beléptetési és kiléptetési szabályzat: Meghatározza a hozzáférési jogosultságok kezdeményezését és visszavonását a felhasználói életciklus eseményeivel összhangban.

10.1.5 P11 – Felhasználóifiók- és jogosultságkezelési szabályzat: Operatív szinten valósítja meg a fiókszintű kontrollokat, és technikai hozzáférés-érvényesítési előírásokkal egészíti ki a jelen szabályzatot.

10.2 Ezek a szabályzatok együtt egységes és kikényszeríthető hozzáférés-irányítási keretrendszert biztosítanak az üzleti területek és technológiák teljes körében.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001:2022:

11.1.1 5.15 pont – Hozzáférés-szabályozás: Jelen szabályzat teljesíti azt a követelményt, hogy az információkhoz és az egyéb kapcsolódó eszközökhöz való hozzáférést üzleti és információbiztonsági követelmények alapján kell szabályozni.

11.1.2 5.17 pont – Identitáskezelés és 5.18 pont – Hitelesítési információk: Ezek végrehajtása identitáskezelési jogosultságkiosztással, hitelesítési mechanizmusokkal és jogosultság-hozzárendelésekkel történik.

11.1.3 A melléklet 8.2 kontrollja (Hozzáférés-szabályozási szabályzat) és 8.3 kontrollja (Identitáskezelés): Ezek adják a jelen szabályzat kontrollcéljainak alapját, beleértve a szerepköralapú hozzáférést, a felhasználói életciklus integrációját és az emelt jogosultságú hozzáférések védelmét.

11.2 NIST SP 800-53 Rev.5:

11.2.1 AC család (AC-1–AC-20): Jelen szabályzat támogatja a NIST fizikai és logikai rendszerekre vonatkozó hozzáférés-szabályozási követelményeit, beleértve a szabályzat meghatározását (AC-1), a fiókkezelést (AC-2) és a feladatkörök elkülönítését (AC-5).

11.2.2 IA család (IA-1–IA-8): Iránymutatást ad az identitáshitelesítéshez, a hitelesítési adatok védelméhez és az MFA alkalmazásához.

11.2.3 AU-2, AU-12: A jelen szabályzat alapján érvényesített naplózási és auditkövetelmények támogatják a felhasználói elszámoltathatóságot és az incidensvizsgálatot.

11.2.4 PE-2–PE-6: A fizikai hozzáférés korlátozására vonatkoznak, amelyeket jelen szabályzat részben beléptetőkártyás kontrollokkal és épület-hozzáférési jogosultságokkal érvényesít.

11.3 GDPR (2016/679):

11.3.1 5. cikk (1) bekezdés f) pont: A személyes adatokat védeni kell a jogosulatlan hozzáféréssel szemben. Jelen szabályzat biztosítja ezen elv technikai és eljárási érvényesítését.

11.3.2 32. cikk (1) bekezdés b) pont: Előírja a hozzáférési kontrollok, a pszeudonimizálás és a titkosítás alkalmazását a személyes adatok jogosulatlan kezelésének megelőzése érdekében.

11.3.3 (39) preambulumbekezdés: Előírja a személyes adatokhoz való hozzáférés minimalizálását, amelyet a jelen szabályzat a legkisebb jogosultság elvével és a hozzáférés indokolásának követelményével érvényesít.

11.4 NIS2 irányelv (2022/2555):

11.4.1 21. cikk (2) bekezdés c)–e) pont: Jelen szabályzat lehetővé teszi a hozzáférés-szabályozásra, a felhasználói hitelesítésre és az eszközvédelemre vonatkozó technikai és szervezési intézkedések alkalmazását az alapvető és fontos szervezeteknél.

11.5 DORA-rendelet (2022/2554):

11.5.1 6. cikk: Olyan IKT-kockázatkezelési szabályzatokat ír elő, amelyek kifejezetten magukban foglalják a felhasználói hozzáférés kezelését és az identitások életciklusára vonatkozó kontrollokat. Jelen szabályzat teljesíti ezt a követelményt a pénzügyi és IKT-szolgáltatási ágazatok számára.

11.5.2 9. cikk (2) bekezdés: Jelen szabályzat támogatja az erős hozzáférési kontrollok érvényesítését a harmadik felek által nyújtott és a csoporton belüli IKT-szolgáltatások kezelésének részeként.

11.6 COBIT 2019:

11.6.1 APO07 – Emberi erőforrások kezelése: Érvényesíti a beléptetési és kiléptetési kontrollokat a hozzáférés-irányítás támogatása érdekében.

11.6.2 BAI03 – Megoldások azonosításának és kialakításának kezelése: Beépíti a hozzáférés-szabályozási követelményeket a rendszertervezésbe és a változáskezelési folyamatokba.

11.6.3 DSS01 – Üzemeltetés kezelése és DSS05 – Biztonsági szolgáltatások kezelése: Szabályozza a logikai hozzáférés korlátozásainak érvényesítését és a szabálysértések nyomon követését.

11.6.4 MEA03 – Megfelelés nyomon követése, értékelése és felmérése: Támogatja a hozzáférés-szabályozás hatékonyságának ellenőrzését szolgáló audit- és bizonyossági mechanizmusokat.