					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P07S					Dokumentum címe: **Beléptetési és kiléptetési 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**

A vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	6.2, 7. pont	HR-biztonsági és tudatossági követelmények
ISO/IEC 27002:2022	6.2, 6.5 kontrollok	Beléptetési és kiléptetési biztonsági gyakorlatok
NIST SP 800-53 Rev.5	PS-4, AC-2, PL-4	Munkaviszony megszűnésének kezelése; hozzáférési életciklus-kezelés; tervezés
EU NIS2	21. cikk (2) bekezdés h) pont	HR-biztonság és hozzáférési életciklus
EU DORA	12. cikk	Hozzáférés-szabályozás és hozzáférés visszavonása az IKT-rendszerek esetében
COBIT 2019	APO07, DSS01	Munkatársi biztonság, logikai és fizikai hozzáférés-szabályozás
EU GDPR	32. cikk	A személyes adatok biztonsága a foglalkoztatás során

1. Cél

1.1 Jelen szabályzat meghatározza az új munkavállalók és szerződéses közreműködők beléptetésének, valamint a kilépés vagy szerepkör-változás esetén szükséges hozzáférés-megszüntetés biztonságos végrehajtásának folyamatát.

1.2 A szabályzat biztosítja, hogy a hozzáférések kiosztása a legkisebb jogosultság elve alapján történjen, valamennyi eszköz nyilvántartásba kerüljön, továbbá a kritikus intézkedések — például a rendszerek deaktiválása és az adatok visszanyerése — haladéktalanul megtörténjenek.

1.3 Jelen szabályzat a strukturált és auditálható beléptetési és kiléptetési tevékenységeken keresztül támogatja a megfelelőséget, a működés folytonosságát és az adatvédelmet.

2. Hatály

2.1 Jelen szabályzat hatálya az alábbiakra terjed ki:

2.1.1 valamennyi állandó és ideiglenes munkavállaló

2.1.2 szerződéses közreműködők, tanácsadók és gyakornokok

2.1.3 rendszer- vagy fizikai hozzáféréssel rendelkező külső szolgáltatók

2.2 A szabályzat az alábbiakat fedi le:

2.2.1 beléptetés: felhasználói fiókok létrehozása, hozzáférések biztosítása, eszközök kiadása

2.2.2 kiléptetés: hozzáférések megszüntetése, vállalati eszközök visszavétele és digitális identitások biztonságos lezárása

2.2.3 belső szerepkör-változások, amelyek a hozzáférések újrakonfigurálását vagy eszközök újrahozzárendelését igénylik

2.3 Jelen szabályzat a hivatalos üzleti tevékenységekhez használt valamennyi eszközre, platformra és helyszínre alkalmazandó.

3. Célkitűzések

3.1 Biztosítani kell, hogy az új munkatársak az ellenőrzött szerepkörök és felelősségi körök alapján kapjanak hozzáférést és erőforrásokat.

3.2 Biztosítani kell, hogy a távozó felhasználók rendszerekhez és létesítményekhez való hozzáférése legkésőbb az utolsó munkanap végéig teljes körűen megszüntetésre kerüljön.

3.3 Meg kell előzni a gazdátlan felhasználói fiókok és a vissza nem szolgáltatott eszközök fennmaradását, mivel ezek biztonsági kockázatot jelentenek.

3.4 Fenn kell tartani a beléptetési, áthelyezési és kiléptetési intézkedések dokumentált nyilvántartását.

3.5 Az ellenőrzőlisták és a szervezeti egységek közötti koordináció alkalmazásával elő kell mozdítani az elszámoltathatóságot.

4. Szerepkörök és felelősségek

4.1 Ügyvezető

4.1.1 Jóváhagyja a kiemelt jogosultságú szerepkörökhöz kapcsolódó hozzáféréseket, és felügyeli a beléptetési és kiléptetési folyamatot.

4.1.2 Biztosítja, hogy a kivételek megfelelően indokoltak legyenek, és helyesbítő intézkedések történjenek, ha a folyamatokat nem tartják be.

4.2 Irodavezető / Humánerőforrás

4.2.1 Kezdeményezi az új belépők beléptetését, és értesíti az IT-t a kilépésekről.

4.2.2 Biztosítja a jogi dokumentumok (pl. titoktartási megállapodás) aláírását, valamint a biztonsági szabályzatok tudomásulvételét.

4.2.3 Fenntartja a beléptetési és kiléptetési ellenőrzőlistákat, és nyomon követi a szabályzat betartását.

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

9. Felülvizsgálati és aktualizálási követelmények

9.1 Éves felülvizsgálat

9.1.1 Jelen szabályzatot az ügyvezetőnek és a HR-/IT-vezetőknek legalább évente egyszer felül kell vizsgálniuk.

9.2 Soron kívüli felülvizsgálatot kiváltó okok

9.2.1 A szabályzatot aktualizálni kell, ha:

9.2.1.1 új HR- vagy IT-rendszerek kerülnek bevezetésre

9.2.1.2 változik a külső IT-szolgáltató vagy a kiszervezett HR-szolgáltatás

9.2.1.3 a biztonsági auditok folyamathiányosságokat tárnak fel

9.2.1.4 változnak a szabályozási kötelezettségek (pl. GDPR-frissítések)

9.2.1.5 kritikus kiléptetési hiba vagy incidens következik be

9.3 Verziókezelés és jóváhagyás

9.3.1 A szabályzat minden verziójának tartalmaznia kell:

9.3.1.1 a verziószámot és a dátumot

9.3.1.2 a változások összefoglalását

9.3.1.3 az ügyvezető jóváhagyását

9.3.1.4 a korábbi verziók archivált példányait, amelyeket legalább három évig meg kell őrizni

9.4 Kommunikáció és tudomásulvétel

9.4.1 A beléptetésért vagy kiléptetésért felelős valamennyi munkatársat értesíteni kell a szabályzat minden módosításáról. Az éves tudatosságnövelő vagy ismétlő eligazítás kötelező.

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzat az alábbi szabályzatokat támogatja, és azok támogatják ezt a szabályzatot:

10.1.1 P2S – Irányítási szerepkörök és felelősségek szabályzat: biztosítja az elszámoltathatóságot a hozzáférési és beléptetési folyamatokban

10.1.2 P4S – Hozzáférés-szabályozási szabályzat: meghatározza a szerepköralapú hozzáférés-kiosztás és deaktiválás technikai megvalósítását

10.1.3 P6S – Kockázatkezelési szabályzat: értékeli a beléptetési és kiléptetési kontrollok hiányosságaiból eredő kockázatokat

10.1.4 P8S – Információbiztonsági tudatossági és képzési szabályzat: előírja a munkatársak beléptetéskori eligazítási követelményeit

10.1.5 P30S – Incidenskezelési szabályzat: biztonsági incidensként kezeli a hozzáférések megszüntetésének elmulasztását vagy az eszközlopást

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 6.2. pont – Meghatározza a HR-biztonsági követelményeket

11.1.2 7.2. pont – Előírja az új munkatársak tudatossági képzését

11.2 ISO/IEC 27002

11.2.1 6.2 és 6.5 kontrollok – Részletezik a munkaviszony kezdetéhez és megszűnéséhez kapcsolódó biztonsági gyakorlatokat

11.3 NIST SP 800-53 Rev. 5

11.3.1 PS-4 – A munkaviszony megszűnésének eljárásai, beleértve a hozzáférések deaktiválását

11.3.2 AC-2 – Biztosítja a felhasználói hozzáférések életciklus-kezelését

11.3.3 PL-4 – Előírja a személyi állomány változásainak tervezését

11.4 EU GDPR

11.4.1 32. cikk – Biztosítja a megfelelő biztonságot a foglalkoztatás alatt és azt követően, különösen a személyes adatokhoz való hozzáférés tekintetében

11.5 EU NIS2 irányelv

11.5.1 21. cikk (2) bekezdés h) pont – Előírja a humánerőforrás-biztonsági és hozzáférési életciklus-kontrollokat

11.6 EU DORA

11.6.1 12. cikk – Előírja, hogy a szabályozott pénzügyi szervezetek szabályozzák a munkatársi hozzáférést az IKT-rendszerekhez, beleértve a visszavonási eljárásokat is

11.7 COBIT 2019

11.7.1 APO07 – Emberi erőforrások kezelése: meghatározza a munkatársi életciklushoz kapcsolódó biztonsági követelményeket

11.7.2 DSS01 – Üzemeltetés kezelése: lefedi a logikai és fizikai hozzáférés szabályozását a foglalkoztatási átmenetek során