					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P07					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**

Vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	7.2. pont, 6. pont	Személyzeti kompetencia, biztonságos integráció, valamint a kilépéssel és változásokkal kapcsolatos felelősségek érvényesítése.
ISO/IEC 27002:2022	6.2., 6.5. és 5. kontrollok	Beléptetési, hozzáférési és a személyzeti életciklushoz kapcsolódó kontrollok.
NIST SP 800-53 Rev.5	PS-4, PS-5, AC-2, AC-6, IA-4, IA-5, CM-5, AU-2, AU-6	Személyi áthelyezés és kiléptetés, a legkisebb jogosultság elve, auditnaplózás, valamint hozzáférés-kezelés a személyzeti változások során és azt követően.
GDPR	5. cikk (1) bekezdés f) pont, 25. cikk, 32. cikk; (39) preambulumbekezdés	Hozzáférés-korlátozás, bizalmas kezelés, védelem és megfelelő kontrollok a személyzeti adatok tekintetében.
NIS2 irányelv	21. cikk (2) bekezdés b), c), d) pont	Személyzeti és működési biztonsági intézkedések; belső fenyegetések mérséklése; életciklus-folyamatok.
DORA-rendelet	5. cikk, 8. cikk, 9. cikk	Irányítás, belső IKT-kontrollok, IKT-kockázatkezelés, incidenskezelés személyzeti átmenetek során.
COBIT 2019	APO07, BAI08, DSS05, MEA03	Humánerőforrás-kezelés, tudáskezelés, valamint biztonság és megfelelés a beléptetés és kiléptetés során.

1. Cél

1.1 Jelen szabályzat egységes eljárásokat határoz meg a beléptetés, a belső áthelyezések és a kiléptetés kezelésére valamennyi felhasználói csoportra kiterjedően.

1.2 Biztosítja a fizikai és logikai hozzáférések időben történő és biztonságos kiadását, illetve visszavonását, valamint a bizalmas kezelés, az elszámoltathatóság és az eszközök visszaszolgáltatásának érvényesítését.

1.3 Jelen szabályzat a HR-, IT- és biztonsági folyamatokba beépített beléptetési és kiléptetési kontrollok alkalmazásával mérsékli a jogosulatlan hozzáférésből, adatszivárgásból és vissza nem szolgáltatott eszközökből eredő kockázatokat.

1.4 Támogatja az ISO/IEC 27001:2022 A. melléklet 6.5. kontrolljának teljesülését azáltal, hogy biztosítja a személyzeti biztonsági kötelezettségek érvényesítését a foglalkoztatási vagy megbízási jogviszony fennállása alatt és annak megszűnését követően is.

2. Hatály

2.1 Jelen szabályzat minden olyan munkavállalóra, vállalkozóra, tanácsadóra, beszállítóra és egyéb harmadik félre vonatkozik, aki hozzáférést kap a szervezet rendszereihez, hálózataihoz, létesítményeihez vagy adataihoz.

2.2 A szabályzat az alábbi teljes életciklusra terjed ki:

2.2.1 Beléptetés (felvétel, szerződéses bevonás vagy ideiglenes megbízás)

2.2.2 Belső áthelyezés vagy szerepkör-változás

2.2.3 Kiléptetés (felmondás, nyugdíjazás, munkaviszony megszűnése, szerződés lejárta)

2.3 A szabályzat az alábbi területekre terjed ki:

2.3.1 Logikai hozzáférés (rendszerek, alkalmazások, felhőszolgáltatások, VPN)

2.3.2 Fizikai hozzáférés (belépőkártyák, kulcsok, épületbeléptető rendszerek)

2.3.3 Kiosztott eszközök (laptopok, telefonok, tokenek, hitelesítő adatok)

2.3.4 Szabályzatok és titoktartási kötelezettségek tudomásulvétele

2.4 Valamennyi szervezeti egység (HR, IT, létesítményüzemeltetés, biztonság, vezetés) köteles a beléptetési és kiléptetési munkafolyamatokban a saját szerepkörének megfelelő feladatokat végrehajtani.

3. Célkitűzések

3.1 Biztosítani, hogy minden érintett kizárólag a biztonsági, képzési és szerződéses előfeltételek teljesítését követően kapjon hozzáférést.

3.2 A szerepkör-változással vagy a jogviszony megszűnésével érintett hozzáférési jogosultságok haladéktalan visszavonása, valamint a szervezeti eszközök visszavétele.

3.3 A szervezeti eszközök bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése a személyi változások során.

3.4 Az auditkészültség és a jogi védhetőség támogatása a beléptetési és kiléptetési események teljes körű nyilvántartásával.

3.5 A belső fenyegetésekből eredő kitettség csökkentése minden, személyzethez kapcsolódó hozzáférési esemény ellenőrzésével és dokumentálásával.

3.6 A szervezet személyzeti életciklusának összehangolása a kockázatalapú biztonsági gyakorlattal és a szabályozói követelményekkel.

4. Szerepkörök és felelősségek

4.1 Felső vezetés

4.1.1 Jóváhagyja jelen szabályzatot, és biztosítja a beléptetési, kiléptetési és hozzáférés-kezelési folyamatokhoz szükséges felhatalmazást és erőforrásokat.

4.1.2 Biztosítja, hogy a személyi változások ne tegyék ki a szervezetet indokolatlan biztonsági vagy jogi kockázatnak.

4.2 Humánerőforrás (HR)

4.2.1 Elindítja a munkavállalók beléptetési és kiléptetési folyamatait, és értesíti az érintett szervezeti egységeket a változásokról.

4.2.2 Biztosítja, hogy az átvilágítások, szerződések, titoktartási megállapodások és szabályzati nyilatkozatok a hozzáférés megadása előtt elkészüljenek, illetve megtörténjenek.

4.2.3 Az értesítési SLA-val összhangban tájékoztatja az IT-t és a létesítményüzemeltetést a munkatársak távozásáról.

4.2.4 A jogi területtel együttműködve koordinálja a jogviszony megszűnését követő kötelezettségek érvényesítését (pl. titoktartási kikötések).

[... 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 szabályzat felülvizsgálatának gyakorisága

9.1.1 Jelen szabályzatot felül kell vizsgálni:

9.1.1.1 Évente, vagy

9.1.1.2 Minden olyan lényeges incidens után, amely hozzáféréssel való visszaélést, eszközvesztést vagy eljárási hibát érint

9.1.1.3 Jelentős HR- vagy IAM-platformváltozások bevezetésekor

9.1.1.4 A személyzeti adatokat vagy kötelezettségeket érintő szabályozási vagy jogi változások esetén

9.2 Felülvizsgálati folyamat és felelősség

9.2.1 A felülvizsgálatot az ISMS vezető és a HR-igazgató koordinálja az IT-biztonság, a jogi terület és a megfelelési terület bevonásával.

9.2.2 Minden módosítást a felső vezetésnek és az ISMS irányító bizottságnak kell jóváhagynia.

9.2.3 A módosított verziókat az érintett szervezeti egységek és személyek részére újbóli tudomásulvétel céljából ismételten ki kell adni.

9.3 Dokumentumkezelés és megőrzés

9.3.1 Jelen szabályzatnak tartalmaznia kell:

9.3.2 Verziókezelés, változástörténet és hatálybalépés dátuma

9.3.3 Felelős tulajdonos és felülvizsgáló(k)

9.3.4 A szabályzat besorolása és jóváhagyási nyilvántartása

9.3.5 Az elavult verziókat a Dokumentumkezelési szabályzattal összhangban legalább 3 évig archiválni kell.

10. Kapcsolódó szabályzatok és összefüggések

10.1.1 Jelen szabályzat közvetlenül az alábbi szabályzatokhoz kapcsolódik:

10.1.2 P1 – Információbiztonsági szabályzat: Meghatározza a szervezet biztonsági célkitűzéseit, beleértve a személyzeti hozzáférések irányítását is.

10.1.3 P4 – Hozzáférés-kezelési szabályzat: Meghatározza a beléptetési és kiléptetési események alapján a rendszer- és fizikai hozzáférések kiadására és visszavonására vonatkozó működési követelményeket.

10.1.4 P3 – Elfogadható használat szabályzata: Előírja a tudomásulvételt a beléptetés során, és támogatja a szabályzat alkalmazását a jogviszony megszűnését követően is.

10.1.5 P6 – Kockázatkezelési szabályzat: Biztosítja, hogy a felhasználói hozzáférési és átmeneti kockázatok értékelése és kezelése az ISMS elveivel összhangban történjen.

10.1.6 P11 – Felhasználói fiók- és jogosultságkezelési szabályzat: Szabályozza a jelen szabályzatot támogató, hozzáférés-létesítéshez és -megszüntetéshez kapcsolódó technikai kontrollokat.

10.2 E szabályzatok együtt integrált kontrollrendszert alkotnak az emberi életciklus-események biztonságos és elszámoltatható kezelésére.

11. Hivatkozott szabványok és keretrendszerek

11.1 Jelen szabályzat a nemzetközileg elismert biztonsági, adatvédelmi és IT-irányítási keretrendszerekkel összhangban készült annak érdekében, hogy a beléptetési és kiléptetési

folyamatok biztonságosak, nyomon követhetők, valamint a jogi és szervezeti követelményeknek megfelelőek legyenek.

11.2 ISO/IEC 27001:

11.2.1 7.2. pont – Kompetencia és 6.2. pont – Információbiztonsági célok: Jelen szabályzat támogatja a személyzeti kompetencia kialakítását és az egyének biztonságos integrálását olyan szerepkörökbe, amelyek hatással vannak az ISMS céljaira.

11.2.2 A. melléklet 6.5. kontroll – Felelősségek a foglalkoztatás megszűnését vagy megváltozását követően: Jelen szabályzat teljes körűen érvényesíti a fennmaradó hozzáférési jogosultságok, az adatkezelői őrzés és a szerződéses kötelezettségek kontrolljait a távozáskor.

11.2.3 A. melléklet 5.9. kontroll – Átvilágítás és 6.2. kontroll – A foglalkoztatás feltételei: A beléptetési eljárások e pontokkal összhangban háttérellenőrzési és szabályzati tudomásulvételi mechanizmusokat tartalmaznak.

11.3 NIST SP 800-53 Rev.5:

11.3.1 PS-4 (Személyi kiléptetés) és PS-5 (Személyi áthelyezés): Jelen szabályzat strukturált módon írja elő a hozzáférési jogosultságok, fizikai belépőkártyák és eszközök megszüntetését vagy módosítását.

11.3.2 AC-2 (Fiókkezelés) és AC-6 (Legkisebb jogosultság): Az előírások biztosítják, hogy a hozzáférések a szerepkörhöz igazodjanak, és szükségtelenné válásuk esetén haladéktalanul visszavonásra kerüljenek.

11.3.3 IA-4 (Azonosítókezelés) és IA-5 (Hitelesítő eszközök kezelése): Támogatja a hitelesítő adatok biztonságos kezelését a személyi változások során és azt követően.

11.3.4 CM-5 (Változtatásokhoz kapcsolódó hozzáférési korlátozások): Megakadályozza a jogosulatlan, kilépést követő módosításokat a kiemelt jogosultságok visszavonásával.

11.3.5 AU-2 és AU-6: A hozzáférési események naplózása és nyomon követhetősége megerősítést nyer az IAM és az auditnyom integrációja révén.

11.4 GDPR (2016/679):

11.4.1 5. cikk (1) bekezdés f) pont: Védi a személyes adatokat a jogosulatlan hozzáféréssel szemben, amelyet jelen szabályzat a kiléptetés során alkalmazott hozzáférés-visszavonással érvényesít.

11.4.2 32. cikk: Megfelelő technikai és szervezeti kontrollokat ír elő a személyes adatok védelmére a foglalkoztatási életciklus teljes időtartama alatt.

11.4.3 25. cikk – Beépített és alapértelmezett adatvédelem: Biztosítja, hogy a beléptetés és kiléptetés magában foglalja az adattakarékosságot, a megőrzést és a jogszerű hozzáférési kontrollokat.

11.4.4 (39) preambulumbekezdés: Hangsúlyozza a hozzáférés korlátozását és a bizalmas kezelést, amelyet jelen szabályzat felépítése támogat.

11.5 NIS2 irányelv (2022/2555):

11.5.1 21. cikk (2) bekezdés b), c), d) pont: Olyan személyzeti és működési biztonsági intézkedéseket ír elő, amelyek kiterjednek a hozzáférés-kezelésre, a belső fenyegetések mérséklésére és az életciklus-folyamatokra; ezek mind megjelennek jelen szabályzatban.

11.6 DORA-rendelet (2022/2554):

11.6.1 5. cikk – Irányítás és belső kontrollok: Jelen szabályzat támogatja az emberi kockázatokhoz és hozzáférés-kezeléshez kapcsolódó belső IKT-irányítást.

11.6.2 8. cikk – IKT-kockázatkezelés: Olyan kontrollokat alkalmaz a személyi változásokra, amelyek kritikus eszközök vagy szabályozott környezetek kitettségét eredményezhetik.

11.6.3 9. cikk – Incidensek osztályozása és kezelése: Biztosítja, hogy a kiléptetéshez kapcsolódó jogsértések megfelelő hozzáférés-megszüntetéssel és eszközkezeléssel jelenthetők és mérsékelhetők legyenek.

11.7 COBIT 2019:

11.7.1 APO07 – Irányított humánerőforrás-kezelés: Meghatározza a beléptetéshez és kiléptetéshez kapcsolódó, irányítási célokhoz igazodó szerepköröket, felelősségeket és életciklus-intézkedéseket.

11.7.2 BAI08 – Tudáskezelés: Erősíti az eljárások dokumentálását, a tudás megőrzését és a kontrollok átadását a foglalkoztatás végén.

11.7.3 DSS05 – Irányított biztonsági szolgáltatások: Előírja a felhasználók deaktiválását, az eszközök kontrollját és az elszámoltathatóságot a szerepköri átmenetek során.

11.7.4 MEA03 – Megfelelés nyomon követése, értékelése és vizsgálata: Biztosítja, hogy a beléptetési és kiléptetési kontrollok értékelése a belső és külső auditok során megtörténjen.