					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P04S					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**

Vonatkozó szabványokkal és jogszabályokkal való összhang

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	5. fejezet	
ISO/IEC 27002:2022	Kontrollok: 5.15, 5.16, 5.17	
NIST SP 800-53 Rev. 5	AC-1–AC-5	
GDPR	32. cikk	
NIS2 irányelv	21. cikk (2) bekezdés b) pont	
DORA-rendelet	9. cikk	
COBIT 2019	APO07, DSS01	

1. Cél

1.1. Jelen szabályzat meghatározza, hogy a szervezet milyen módon kezeli a rendszerekhez, adatokhoz és létesítményekhez való hozzáférést annak biztosítása érdekében, hogy az információkhoz kizárólag az arra jogosult személyek férhessenek hozzá, üzleti szükségesség alapján.

1.2. A szabályzat egyértelmű követelményeket állapít meg a felhasználói hozzáférések létrehozására, módosítására, nyomon követésére és megszüntetésére annak érdekében, hogy csökkenjen a jogosulatlan hozzáférés kockázata, és biztosított legyen a vonatkozó jogszabályoknak és szabványoknak való megfelelés.

1.3. A szabályzat előírja a legkisebb jogosultság elvének alkalmazását, amely szerint a hozzáférést a munkaköri feladatok ellátásához feltétlenül szükséges minimumra kell korlátozni.

2. Hatály

2.1. Jelen szabályzat kiterjed minden olyan személyre, aki a szervezet informatikai rendszereihez, hálózataihoz, adataihoz vagy létesítményeihez való hozzáférést használja vagy kezeli, beleértve az alábbiakat:

2.1.1. Munkavállalók

2.1.2. Vállalkozók

2.1.3. Ideiglenes munkavállalók

2.1.4. Külső informatikai szolgáltatók

2.2. A szabályzat az alábbi hozzáférésekre terjed ki:

2.2.1. Vállalati alkalmazások, fájlmegosztások és adatbázisok

2.2.2. E-mail-, VPN- és távelérési rendszerek

2.2.3. Üzleti célra használt felhőszolgáltatások

2.2.4. Fizikai hozzáférés védett területekhez, például irodákhoz vagy szervertermekhez

2.3. Jelen szabályzat valamennyi eszközre (vállalati tulajdonú vagy jóváhagyott BYOD-eszközre), platformra és helyszínre érvényes és alkalmazandó.

3. Célkitűzések

3.1. Biztosítani kell, hogy hozzáférési jogosultság kizárólag szerepkör és üzleti indoklás alapján, formális jóváhagyást követően adható.

3.2. Meg kell akadályozni az érzékeny adatokhoz, rendszerekhez vagy infrastruktúrához való jogosulatlan vagy túlzott hozzáférést.

3.3. Egyértelmű eljárásokat kell meghatározni a felhasználói hozzáférések létrehozására, módosítására és megszüntetésére.

3.4. Elő kell írni a hozzáférések rendszeres felülvizsgálatát, valamint az automatizált vagy manuális naplózást az auditok támogatása érdekében.

3.5. Támogatni kell a hozzáférési korlátozások technikai érvényesítését konfigurációs beállításokkal és nyomon követéssel.

4. Szerepkörök és felelősségi körök

4.1. Ügyvezető

4.1.1. Jóváhagyja a jelen szabályzatot, és biztosítja a hatékony hozzáférés-szabályozás bevezetéséhez szükséges erőforrásokat.

4.1.2. Jóváhagyja a kivételeket, és felülvizsgálja az éves hozzáférési auditok eredményeit.

4.2. Informatikai vezető / külső informatikai szolgáltató

4.2.1. Végzi a felhasználói fiókok létrehozását, módosítását és megszüntetését.

4.2.2. Hozzáférés-szabályozási nyilvántartást vezet valamennyi tevékenységről (létrehozás, módosítás, megszüntetés).

4.2.3. Bevezeti a szerepköralapú hozzáférés-szabályozást (RBAC), és érvényesíti az erős hitelesítést, például a többtényezős hitelesítést (MFA).

4.2.4. Felülvizsgálja a hozzáférési naplókat a gyanús tevékenységek azonosítása érdekében, és az észlelt problémákat jelenti az ügyvezetőnek.

[... 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 szabályzat-felülvizsgálat

9.1.1. Az informatikai vezető köteles a jelen szabályzatot évente felülvizsgálni. A jogi, technikai vagy szervezeti környezet bármely változása esetén a szabályzatot haladéktalanul aktualizálni kell.

9.2. Felülvizsgálatot kiváltó események

9.2.1. A szabályzatot az alábbi esetek bármelyikének bekövetkezésekor is felül kell vizsgálni:

9.2.2. Jelentős rendszerátalakítások vagy felhőmigrációk

9.2.3. A szerepkörök vagy a szervezeti struktúra változása

9.2.4. Jogosulatlan hozzáféréssel összefüggő biztonsági incidens

9.2.5. Szabályozási változások (pl. a GDPR, a NIS2 vagy a DORA módosításai)

9.3. Változások dokumentálása és kommunikálása

9.3.1. A módosításokat verziótörténettel együtt naplózni kell, azokat az ügyvezetőnek jóvá kell hagynia, és az érintett személyekkel közölni kell.

9.4. Elérhetőség és képzés

9.4.1. A jelen szabályzatot minden munkatárs számára elérhetővé kell tenni, és a releváns képzést a beléptetés részeként, majd azt követően évente biztosítani kell.

10. Kapcsolódó szabályzatok és összefüggések

10.1. A jelen szabályzatot az alábbi SME szabályzatokkal összhangban kell alkalmazni a biztonságos hozzáférési gyakorlat teljes körű érvényesítése érdekében:

10.1.1. P3S – Elfogadható használati szabályzat: Biztosítja, hogy a felhasználók megértsék a biztosított hozzáféréssel kapcsolatos elfogadható magatartási elvárásokat.

10.1.2. P5S – Változáskezelési szabályzat: Biztosítja, hogy a hozzáférési jogosultságok összhangban legyenek a jóváhagyott rendszerváltozásokkal.

10.1.3. P7S – Beléptetési és kiléptetési szabályzat: Meghatározza a felhasználói hozzáférések létrehozását és megszüntetését kiváltó eseményeket.

10.1.4. P17S – Adatvédelmi és személyesadat-védelmi szabályzat: Biztosítja, hogy a hozzáférés-szabályozási intézkedések összhangban legyenek a személyes adatok védelmére vonatkozó előírásokkal.

10.1.5. P30S – Incidenskezelési szabályzat: Meghatározza a hozzáféréssel kapcsolatos incidensek (pl. visszaélés vagy adatsértés) kezelésének és kivizsgálásának módját.

11. Hivatkozott szabványok és keretrendszerek

11.1. ISO/IEC 27001

11.1.1. 5.15. kontroll – Előírja a formalizált hozzáférés-szabályozási szabályzatok és folyamatok kialakítását.

11.2. ISO/IEC 27002

11.2.1. 5.15–5.17. kontrollok – Részletes útmutatást adnak a szerepköralapú hozzáférésre, a felhasználói életciklus kezelésére és az emelt jogosultságú hozzáférések kezelésére vonatkozóan.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AC-1–AC-5 – Strukturált hozzáférés-kezelési szabályzatokat írnak elő, beleértve a fiókok jóváhagyását, felülvizsgálatát és nyomon követését.

11.4. GDPR

11.4.1. 32. cikk – Előírja az adatbiztonság és a bizalmasság biztosításához szükséges technikai és szervezési intézkedéseket, ideértve a hozzáférés-kezelést is.

11.5. NIS2 irányelv

11.5.1. 21. cikk (2) bekezdés b) pont – Előírja az operatív hozzáférés-szabályozási és identitáskezelési rendszerek alkalmazását a jogosulatlan rendszerhozzáférés megelőzése érdekében.

11.6. DORA-rendelet

11.6.1. 9. cikk – Hangsúlyozza az IKT-kockázatok biztonságos kezelését, beleértve a pénzügyi szervezetekre vonatkozó erős hozzáférés-szabályozást is.

11.7. COBIT 2019

11.7.1. APO07 – Menedzselt humánerőforrás: Meghatározott és érvényesített hozzáférési felelősségi köröket követel meg.

11.7.2. DSS01 – Működésirányítás: Magában foglalja a logikai hozzáférés kezelésére és a biztonságos működési környezet fenntartására vonatkozó eljárásokat.