	Ide írja be a bejegyzett jogi személy nevét
Dokumentumszám: P10S	Dokumentum címe: **Tiszta asztal és képernyő 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	7.2, 8. pont	
ISO/IEC 27002:2022	7. kontroll	
NIST SP 800-53 Rev.5	PE-2, AC-11	
EU NIS2	21. cikk (2) d) pont	
EU DORA	9. cikk (2) f) pont	
COBIT 2019	DSS01.06, DSS05	
EU GDPR	32. cikk	

1. Cél

1.1 Jelen szabályzat kötelező érvényű előírásokat határoz meg a biztonságos munkakörnyezet fenntartására annak biztosítása érdekében, hogy az asztalokon, munkaállomásokon és képernyőkön felügyelet nélkül hagyott állapotban ne maradjanak látható bizalmas információk.

1.2 Elsődleges célja annak megelőzése, hogy érzékeny információkhoz jogosulatlan hozzáférés történjen őrizetlenül hagyott nyomtatott anyagok, zárolatlan képernyők vagy nem megfelelően tárolt cserélhető adathordozók révén, mind a fizikai irodai környezetben, mind a távoli munkavégzés helyszínein.

1.3 A jelen szabályzatban meghatározott tiszta asztal és képernyő gyakorlat csökkenti a megelőzhető kitettségi kockázatokat, ezáltal erősíti a szervezet képességét az ISO/IEC 27001 tanúsítási követelményeinek teljesítésére. E gyakorlatok azt is igazolják az ügyfelek, partnerek és auditorok felé, hogy szervezetünk az információbiztonságot erőforrás-korlátozott környezetben is komolyan veszi.

1.4 Jelen szabályzat támogatja az elszámoltathatóság és a tudatosság kultúráját, biztosítva, hogy valamennyi munkatárs – szerepkörétől vagy technikai szaktudásától függetlenül – tisztában legyen a vállalati és ügyfélinformációk vizuális kitettséggel, eltulajdonítással vagy elvesztéssel szembeni védelmére vonatkozó felelősségével.

2. Hatály

2.1 Jelen szabályzat az alábbiakra terjed ki:

2.1.1 valamennyi munkavállalóra, szerződéses közreműködőre, gyakornokra és ideiglenes munkatársra, akik vállalati tulajdonú vagy számukra kijelölt munkaállomást, íróasztalt vagy mobileszközt használnak;

2.1.2 valamennyi fizikai helyszínre, ahol üzleti tevékenység folyik, beleértve a dedikált irodákat, a közös munkavégzési környezeteket és a távoli vagy otthoni munkavégzés helyszíneit;

2.1.3 valamennyi, megjelenítésre alkalmas digitális eszközre, beleértve az asztali számítógépeket, laptopokat, táblagépeket és üzleti célra használt külső monitorokat.

2.2 A szabályzat kiterjed minden olyan fizikai vagy digitális vagyonelemre, amely érzékeny információt megjeleníthet, tartalmazhat vagy továbbíthat, ideértve az alábbiakat:

2.2.1 nyomtatott nyilvántartások vagy kézzel írt jegyzetek;

2.2.2 USB-meghajtók, CD-k és külső merevlemezek;

2.2.3 üzleti üzenetküldésre vagy e-mail használatára szolgáló mobiltelefonok;

2.2.4 a munkavégzéshez használt rendszerekhez csatlakoztatott számítógép-monitorok és projektorok.

2.3 Jelen szabályzat a rendes munkaidőn kívül és nem szokásos működési helyzetekben is alkalmazandó, például munkaidőn túli karbantartás vagy vészhelyzeti reagálási tevékenység során.

3. Célkitűzések

3.1 Olyan gyakorlati és következetes kontrollok alkalmazása, amelyek biztosítják, hogy az asztalokon, képernyőkön vagy közös használatú terekben ne maradjon szabadon hozzáférhető érzékeny információ.

3.2 A jogosulatlan hozzáférés kockázatának minimalizálása mind belső forrásokból eredően (pl. más munkavállalók nem szándékos hozzáférése), mind külső fenyegetések esetén (pl. látogatók, takarítószemélyzet vagy vállalkozók).

3.3 A fizikai és logikai hozzáférés-korlátozás támogatása annak előírásával, hogy a munkatársak aktívan gondoskodjanak a munkavégzéshez használt anyagok védelméről, és távollét esetén zárolják számítógépüket.

3.4 A biztonságos munkavégzési gyakorlatokkal kapcsolatos tudatosság erősítése, valamint egyszerűen alkalmazható és betartható szabályok meghatározása a napi működéshez, a munkavégzés helyétől függetlenül.

3.5 Annak biztosítása, hogy a szabályzat összhangban legyen az ISO/IEC 27001 A melléklet 7.7. kontrolljával és az ISO/IEC 27002 szerinti bevezetési útmutatással a tiszta asztal és képernyő követelményei tekintetében.

3.6 Annak biztosítása, hogy a szervezet vállalati szintű infrastruktúra nélkül is igazolni tudja a kellő gondosságot és az auditra való felkészültséget.

4. Szerepkörök és felelősségi körök

4.1 Ügyvezető

4.1.1 A szabályzat tulajdonosa, és biztosítja annak megfelelő kommunikálását, megértését és betartását valamennyi munkavállaló és szerződéses közreműködő részéről.

4.1.2 Felelős a kivételek jóváhagyásáért, a szabálysértések kezeléséért, valamint a biztonságos munkavégzési gyakorlatokhoz kapcsolódó képzések felügyeletéért.

4.1.3 Köteles rendszeres ellenőrzéseket végezni vagy azokat delegálni – legalább negyedévente – annak megerősítésére, hogy a fizikai és digitális munkaterületek megfelelnek a szabályzat előírásainak.

4.2 Kijelölt munkavállaló (amennyiben kijelölésre került)

4.2.1 Felelős lehet a technikai beállítások bevezetéséért (pl. képernyőzár időtúllépési beállításai), illetve fizikai tárolóeszközök biztosításáért (pl. zárható fiókok).

4.2.2 Támogatja az ügyvezetőt a nemmegfelelőségek jelentésében, a munkaterületi biztonsági emlékeztetők kezelésében, valamint a helyesbítő intézkedések nyomon követésében, ha problémák kerülnek azonosításra.

4.2.3 Közreműködik annak biztosításában, hogy minden munkavállaló – ahol ez megvalósítható – megfelelő zárható tárolási megoldásokhoz vagy biztonságos tárolóhelyekhez férjen hozzá.

[... 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 Az ügyvezető köteles a jelen szabályzatot legalább évente egyszer, valamint az alábbi események bármelyikét követően felülvizsgálni:

9.1.1 új irodai terek, eszközök vagy közös rendszerek bevezetése;

9.1.2 az alkalmazandó jogi vagy tanúsítási követelmények változása;

9.1.3 auditokból, kockázatértékelésekből vagy biztonsági incidensekből származó megállapítások.

9.2 A soron kívüli módosításokat e-mailben kell kommunikálni valamennyi munkavállaló felé, és azok tudomásulvétele kötelező.

9.3 Jelen szabályzat korábbi verzióit biztonságosan kell tárolni, és auditálható módon kell megőrizni annak igazolására, hogy a szabályzat folyamatosan összhangban áll az ISO/IEC 27001 szabvánnyal és a kapcsolódó keretrendszerekkel.

10. Kapcsolódó szabályzatok és összefüggések

10.1 P2S – Irányítási szerepkörök és felelősségek szabályzata: tisztázza az ügyvezető jogosultságát a fizikai és digitális munkaterületi magatartás betartatására és auditálására.

10.2 P4S – Hozzáférés-szabályozási szabályzat: támogatja a képernyőzárolás és a biztonságos munkaállomás-bejelentkezési gyakorlat technikai megvalósítását.

10.3 P8S – Információbiztonsági tudatossági és képzési szabályzat: megerősíti a szabályzatnak való megfeleléshez szükséges viselkedésalapú képzést.

10.4 P17S – Adatvédelmi és a magánszféra védelmére vonatkozó szabályzat: meghatározza a személyes és érzékeny adatok kezelésére és védelmére vonatkozó kötelezettségeket a GDPR-nak megfelelően.

10.5 P30S – Incidenskezelési szabályzat: meghatározza az eszkalációs és reagálási keretrendszert arra az esetre, ha egy szabályszegés adat-kitettséget vagy incidenst eredményez.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 7.2. pont: előírja, hogy valamennyi munkatárs legyen tisztában a biztonsági felelősségeivel, beleértve a fizikai védelmi intézkedéseket is.

11.1.2 8.1. pont: az operatív kontrolloknak megfelelő fizikai és logikai védelmet kell biztosítaniuk.

11.2 ISO/IEC 27002

11.2.1 7.7. kontroll: részletes útmutatást ad a tiszta asztal és képernyő követelményeinek kialakításához, kommunikálásához és alkalmazásához.

11.3 NIST SP 800-53 Rev.5

11.3.1 PE-2: meghatározza a fizikai hozzáférés-szabályozás elvárásait, beleértve a munkatársak magatartását a védett környezetekben.

11.3.2 AC-11: előírja a munkamenet-zárolási funkcionalitást a munkaállomásokon a jogosulatlan megtekintés vagy interakció megelőzése érdekében.

11.4 EU GDPR

11.4.1 32. cikk: előírja, hogy a szervezetek fizikai és technikai védelmi intézkedésekkel védjék a személyes adatokat, beleértve a munkaállomásokat és dokumentumokat is.

11.5 EU NIS2 irányelv

11.5.1 21. cikk (2) d) pont: előírja a szervezetek számára a kockázatalapú fizikai és logikai hozzáférés-szabályozási szabályzatok bevezetését.

11.6 EU DORA

11.6.1 9. cikk (2) f) pont: előírja az IKT-biztonsági szabályzatokat, beleértve a biztonságos munkaterületi gyakorlatokat, a pénzügyi szektor szereplői és ellátási láncaik számára.

11.7 COBIT 2019

11.7.1 DSS01.06: előírja az eszközök védelmére vonatkozó gyakorlatokat, beleértve a munkaterületekre és adathordozókra vonatkozó fizikai kontrollokat.

11.7.2 DSS05.02: támogatja a végfelhasználói biztonsági gyakorlatok alkalmazását a működési környezetekben.