					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P10					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	6.1.3 pont, 8. fejezet	kockázatkezelési terv, operatív tervezés, valamint a biztonságos munkaterületekre vonatkozó kontrollok
ISO/IEC 27002:2022	7. kontroll	a felügyelet nélkül hagyott fizikai információk védelmét szolgáló magatartási és környezeti kontrollok
NIST SP 800-53 Rev.5	PE-2, PS-7, MP-6, AC-11, CM-6, IA-5	fizikai hozzáférés, külső személyzet biztonsága, adathordozók megsemmisítése, munkamenet-zárolás, konfigurációs és hitelesítési kontrollok
GDPR	5. cikk (1) bekezdés f) pont, 32. cikk, (39) preambulumbekezdés	adatintegritás, bizalmasság, valamint a fizikai adatvédelemhez kapcsolódó védelmi intézkedések
NIS2 irányelv	21. cikk (2) bekezdés d) pont, 21. cikk (3) bekezdés	a fizikai biztonságra, a felhasználói magatartásra és az adatszivárgás megelőzésére vonatkozó szabályzatok
DORA-rendelet	5. cikk, 8. cikk, 9. cikk	belső irányítás, IKT-kockázatkezelés és a fizikai biztonságot is érintő incidenskezelés
COBIT 2019	DSS01, DSS05, MEA	irányított üzemeltetés, biztonsági szolgáltatások és a megfelelés nyomon követése

1. Cél

1.1 Jelen szabályzat kötelező kontrollokat határoz meg az érzékeny információk védelme érdekében azáltal, hogy előírja a fizikai dokumentumok, munkaállomások, képernyők és cserélhető adathordozók biztonságos kezelését irodai és megosztott munkaterületi környezetben egyaránt.

1.2 A szabályzat támogatja az ISO/IEC 27001 A. melléklet 7.7. kontrollját azzal, hogy olyan magatartási és technikai gyakorlatokat ír elő, amelyek mérséklik a felügyelet nélkül hagyott vagy látható információkból eredő jogosulatlan nyilvánosságra hozatal, eltulajdonítás vagy adatvesztés kockázatát.

1.3 A szabályzat erősíti a fizikai és információbiztonságot a napi működés során, valamint támogatja az alkalmazandó jogi, szerződéses és szabályozási kötelezettségek teljesítését.

2. Hatály

2.1 Jelen szabályzat valamennyi olyan munkatársra alkalmazandó, aki fizikai munkaterületeken dolgozik, vagy azokhoz hozzáfér, ideértve az alábbiakat:

2.1.1 állandó és ideiglenes munkavállalók

2.1.2 vállalkozók, tanácsadók, beszállítók és gyakornokok

2.1.3 harmadik fél szolgáltatói és helyszíni látogatók, akik érzékeny információkhoz férhetnek hozzá

2.2 A követelmények az alábbi helyszínekre terjednek ki:

2.2.1 egyéni irodák, fülkék és nyitott terű munkaterületek

2.2.2 tárgyalók és megosztott együttműködési terek

2.2.3 nyomtatóállomások, recepciós pultok és másolószobák

2.2.4 olyan területek, ahol távoli munkaállomásokat vagy megosztott kioszkokat használnak

2.3 Jelen szabályzat kiterjed az ideiglenes vagy hibrid munkakörnyezetekre is (pl. hot-desking), valamint azokra a nyilvánosan hozzáférhető környezetekre, ahol fennáll a váll fölötti betekintés vagy a felügyelet nélkül hagyott adatok kockázata.

3. Célkitűzések

3.1 Megakadályozni a fizikai vagy digitális formában hozzáférhetően hagyott bizalmas, érzékeny vagy szabályozott adatokhoz történő jogosulatlan hozzáférést.

3.2 Előmozdítani az egységes kockázati profil kialakítását valamennyi munkakörnyezetben fizikai védelmi intézkedések, a munkaállomások beállításai és a végfelhasználói magatartás révén.

3.3 Csökkenteni a gondatlanságból vagy figyelmetlenségből eredő adatvédelmi incidensek, a szellemi tulajdon elvesztése és az adatszivárgás kockázatát.

3.4 Beépíteni a tiszta asztal és tiszta képernyő elveit a szervezeti kultúrába az operatív fegyelem, az auditálhatóság és a jogi védelem támogatása érdekében.

3.5 Támogatni az ISO/IEC 27001, a GDPR 32. cikke, a NIS2 15. cikke, valamint a kritikus vagy személyes adatokra vonatkozó egyéb fizikai biztonsági követelmények teljesítését.

4. Szerepkörök és felelősségi körök

4.1 Felső vezetés

4.1.1 Jóváhagyja e szabályzatot, és támogatja a biztonságtudatos kultúrát valamennyi üzleti egységben.

4.1.2 Megfelelő erőforrásokat biztosít a szabályzat végrehajtásához, a tudatosságnövelő kampányokhoz és a fizikai kontrollokhoz.

4.2 Információbiztonsági vezető / IBIR-vezető

4.2.1 A szabályzat tulajdonosa, és biztosítja annak összhangját az ISO/IEC 27001:2022 követelményeivel, az auditkövetelményekkel és a kockázatkezelési stratégiákkal.

4.2.2 Tudatosságnövelő programokat és kontrollokat alakít ki annak érdekében, hogy a szabályzat a létesítményekben és a hibrid munkavégzési környezetekben egységesen érvényesüljön.

4.2.3 Együttműködik a létesítményüzemeltetési és az IT-területtel annak biztosítása érdekében, hogy a megfelelő fizikai védelmi intézkedések rendelkezésre álljanak.

[... 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 A szabályzat felülvizsgálati ütemezése

9.1.1 Jelen szabályzatot felül kell vizsgálni:

9.1.1.1 legalább évente egyszer

9.1.1.2 minden, a munkaterületet vagy a képernyőn történő hozzáférhetővé válást érintő audit során azonosított meg nem felelés után

9.1.1.3 fizikai vagy környezeti incidens bekövetkezését követően (pl. eszközlopás, jogosulatlan követéses bejutás, megfigyelés)

9.1.1.4 új irodai elrendezések, létesítményi szabályok vagy munkaterületi modellek bevezetésekor (pl. hot-desking, távoli munkahubok)

9.2 Felelős tulajdonosok

9.2.1 A szabályzat tulajdonosa az információbiztonsági vezető vagy a kijelölt IBIR-vezető.

9.2.2 A felülvizsgálati folyamatba az alábbiakat kell bevonni:

9.2.2.1 létesítményüzemeltetési és vállalati biztonsági csapatok

9.2.2.2 IT és infrastruktúra az eszközökhöz kapcsolódó végrehajtás érdekében

9.2.2.3 HR, valamint jogi és megfelelőségi terület a magatartási végrehajtás és a fegyelmi összhang biztosítása érdekében

9.2.3 Minden szabályzatmódosítást verziókezeléssel kell kezelni, az IBIR irányító bizottságának jóvá kell hagynia, és szükség esetén ismételt tudomásulvétellel újra ki kell hirdetni.

9.3 A változások kommunikálása

9.3.1 A felhasználókat az érdemi módosításokról az alábbi csatornákon kell tájékoztatni:

9.3.1.1 intranetes szabályzati központ vagy portál

9.3.1.2 célzott e-mail-kommunikációk

9.3.1.3 beléptetési és ismétlő tájékoztatások, valamint negyedéves eligazítások

9.3.1.4 kötelező tudomásulvételi felhívások minden új, kritikus végrehajtási rendelkezés esetén

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzat összhangban áll az alábbi dokumentumokkal, és támogatja azok céljait:

10.1.1 P1 – Információbiztonsági szabályzat: meghatározza a jelen szabályzat alapját képező felhasználói magatartási és fizikai biztonsági elvárásokat.

10.1.2 P3 – Elfogadható használati szabályzat: szabályozza a felhasználók elszámoltathatóságát az adatok és rendszerek, beleértve a fizikai környezetek védelmét is.

10.1.3 P6 – Kockázatkezelési szabályzat: a fizikai munkaterületi kockázatokat a szervezetszintű információkockázat-elemzés részeként kezeli.

10.1.4 P12 – Eszközkezelési szabályzat: támogatja az asztalon hagyott eszközök és adathordozók nyomon követését és biztonságos kezelését.

10.1.5 P13 – Adatosztályozási és címkézési szabályzat: kapcsolódik a „Bizalmas” vagy „Belső felhasználásra” jelölésű fizikai dokumentumokra vonatkozó tiszta asztal követelményekhez.

10.1.6 P14 – Adatmegőrzési és megsemmisítési szabályzat: iránymutatást ad a fizikai dokumentumok megőrzésére, iratmegsemmisítésére és a gyűjtők kezelésére vonatkozóan.

10.1.7 P22 – Naplózási és felügyeleti szabályzat: alkalmazható a munkaállomások zárolási állapotának, inaktivitási idejének vagy – ahol ez megengedett – a munkaterületi kameraképek felügyeletére.

10.2 E kapcsolódó szabályzatok integrált biztonsági kultúrát teremtenek, amely a felhasználói tudatosságot, a fizikai védelmi intézkedéseket és az elszámoltathatóságot ötvözi a reziliens munkaterületek biztosítása érdekében.

11. Hivatkozott szabványok és keretrendszerek

11.1 Jelen szabályzat összhangban áll olyan nemzetközileg elismert szabványokkal és jogi követelményekkel, amelyek előírják az érzékeny információk védelmét fizikai környezetben és a felhasználói magatartás szintjén.

11.2 ISO/IEC 27001

11.2.1 6.1.3 pont – kockázatkezelési terv: támogatja a fizikai és környezeti kockázatok csökkentését szolgáló kontrollok bevezetését, beleértve a nyitott munkaterületeken tanúsított felhasználói magatartáshoz kapcsolódó kockázatokat is.

11.2.2 8.1 pont – operatív tervezés és kontroll: operatív védelmi intézkedéseket határoz meg a biztonságos munkaterületek és a berendezések használatának kezelésére.

11.3 ISO/IEC 27002:2022 – 7. kontroll

11.3.1 Ez a kontroll olyan magatartási és környezeti védelmi intézkedéseket ír elő, amelyek megelőzik az információkhoz való jogosulatlan hozzáférést a felügyelet nélkül hagyott adathordozók, képernyők vagy nyomtatott anyagok révén. Jelen szabályzat kikényszeríti a fizikai munkaterület rendezettségét, a képernyőzár használatát és az érzékeny dokumentumok megsemmisítését.

11.4 NIST SP 800-53 Rev.5

11.4.1 PE-2 (fizikai hozzáférési jogosultságok): a munkaterületi korlátozások és a zárt tárolás előírása révén kapcsolódik a magas kockázatú környezetekhez.

11.4.2 PS-7 (külső személyzet biztonsága): a vállalkozókra és harmadik fél felhasználóira is kiterjesztett tiszta asztal és tiszta képernyő követelmények révén valósul meg.

11.4.3 MP-6 (adathordozók tisztítása) és AC-11 (munkamenet-zárolás): a biztonságos megsemmisítési eljárásokkal és a kötelező képernyőzár-időzítőkkel kerülnek bevezetésre.

11.4.4 CM-6 (konfigurációs beállítások) és IA-5 (hitelesítő adatok kezelése): támogatják a képernyőzárolás és a munkamenet-kezelés technikai kikényszerítését a végpontokon.

11.5 GDPR (2016/679)

11.5.1 5. cikk (1) bekezdés f) pont: előírja a személyes adatok sértetlenségét és bizalmasságát, beleértve a fizikai hozzáférhetővé válás vagy jogosulatlan megtekintés elleni védelmet is.

11.5.2 32. cikk – Az adatkezelés biztonsága: megfelelő fizikai és szervezeti intézkedések alkalmazását írja elő a személyes adatok véletlen vagy jogellenes megsemmisülése, elvesztése vagy jogosulatlan nyilvánosságra hozatala elleni védelem érdekében, amelyet az asztali és képernyőkontrollok támogatnak.

11.5.3 (39) preambulumbekezdés: előírja, hogy a személyes adatokhoz való hozzáférést a jogosult személyekre kell korlátozni; ez magában foglalja a felügyelet nélkül hagyott fizikai formában rendelkezésre álló adatok biztonságos kezelését is.

11.6 NIS2 irányelv (2022/2555)

11.6.1 21. cikk (2) bekezdés d) pont: a fizikai és környezeti biztonsághoz kapcsolódó szabályzatok és eljárások meglétét írja elő, beleértve a munkahelyi szintű információbiztonsági védelmi intézkedéseket is.

11.6.2 21. cikk (3) bekezdés: olyan biztonsági kultúrát ösztönöz, amely magában foglalja a megfelelő felhasználói magatartást, a tudatosságot és a nem szándékos adatszivárgások megelőzését, amelyet e szabályzat magatartási kontrolljai támogatnak.

11.7 DORA-rendelet (2022/2554)

11.7.1 5. cikk – belső irányítás és kontroll: előírja, hogy minden IKT-val kapcsolatos kockázatot, beleértve az emberi és környezeti fenyegetéseket is, kikényszeríthető szabályzatok útján kell kezelni.

11.7.2 8. cikk – IKT-kockázatkezelés: védelmi intézkedéseket ír elő digitális és fizikai környezetben egyaránt, biztosítva, hogy a távoli, fióki és helyszíni felhasználók ne hozzanak létre kezeletlen kitettséget.

11.7.3 9. cikk – incidenskezelés: előírja, hogy a környezeti vagy magatartási hiányosságokat, amelyek adatok hozzáférhetővé válásához vezetnek, naplózni, osztályozni és megfelelő helyesbítő intézkedésekkel kezelni kell.

11.8 COBIT 2019

11.8.1 DSS01 – irányított üzemeltetés: ismételhető kontrollok révén biztosítja az operatív fegyelmet a fizikai munkaterületek és rendszerek védelmében.

11.8.2 DSS05 – Biztonsági szolgáltatások kezelése: támogatja az adatok, eszközök és hozzáférési végpontok védelmét olyan magatartásalapú végrehajtás útján, mint a tiszta asztal gyakorlata.

11.8.3 MEA03 – a megfelelés monitorozása, értékelése és felmérése: ösztönzi a fizikai védelmi intézkedések és a szabályzatok napi üzleti gyakorlatba történő beépülésének auditálását.