					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P29S					Dokumentum címe: **Tesztadatok és tesztkörnyezetek szabályzata**							
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	6.1., 8. pont	
ISO/IEC 27002:2022	8.28–8.29. kontrollok	
NIST SP 800-53 Rev.5	SA-11, SA-12, SC-32	
GDPR	5. cikk (1) bekezdés c) pont, 25. cikk, 32. cikk	
NIS2 irányelv	21. cikk (2) bekezdés e), h) pont	
DORA-rendelet	9. cikk	
COBIT 2019	BAI07, DSS05	

1. Cél

1.1 Jelen szabályzat meghatározza a tesztadatok és tesztkörnyezetek kezelésének követelményeit annak érdekében, hogy a tesztelési tevékenységek során megelőzhető legyen a véletlen adatkitettség, az adatvédelmi incidens vagy a működési zavar.

1.2 A szabályzat biztosítja, hogy valódi ügyféladatok szoftver- vagy rendszer-tesztelés során ne kerüljenek nem megfelelő felhasználásra, továbbá hogy a tesztkörnyezetek logikailag és technikailag elkülönüljenek az éles rendszerektől.

1.3 A szabályzat célja, hogy támogassa a KKV-kat az ISO/IEC 27001 tanúsítási követelményeknek és a vonatkozó adatvédelmi jogszabályoknak való megfelelésben, ugyanakkor a dedikált IT-csapattal nem rendelkező szervezetek számára is gyakorlatias és végrehajtható maradjon.

2. Hatály

2.1 Jelen szabályzat az alábbiakra terjed ki:

2.1.1 valamennyi tesztkörnyezetre (pl. előéles szerverek, sandbox környezetek, fejlesztési tesztkörnyezetek)

2.1.2 valamennyi tesztadatra, függetlenül attól, hogy manuálisan létrehozott, generált vagy éles adatokból származtatott adatról van szó

2.1.3 a tesztelési tevékenységekben részt vevő valamennyi munkatársra, beleértve a munkavállalókat, vállalkozókat, szabadúszókat és IT-szolgáltatókat

2.1.4 minden olyan tesztelésre, amely hatással lehet ügyféloldali platformokra, belső üzleti rendszerekre vagy harmadik fél szolgáltatásaira

2.2 A szabályzat kiterjed továbbá az alábbiak támogatására használt technikai környezetekre és folyamatokra is:

2.2.1 weboldalak, alkalmazások és eszközök fejlesztése

2.2.2 rendszerfrissítések, konfigurációtesztelés és integrációs tesztelés

2.2.3 automatizált és manuális funkcionális vagy biztonsági tesztek

3. Célkitűzések

3.1 Meg kell akadályozni, hogy a tesztelés során valódi, azonosításra alkalmas ügyféladatok kerüljenek felhasználásra, kivéve, ha azok anonimizáltak, és erre kifejezett jóváhagyás áll rendelkezésre.

3.2 Fenn kell tartani a teszt- és éles rendszerek szigorú elkülönítését a nem szándékolt adatkitettség vagy működési beavatkozás elkerülése érdekében.

3.3 A tesztrendszereket és tesztadatokat megfelelő kontrollokkal védeni kell a jogosulatlan hozzáféréstől, a véletlen közzétételtől, valamint a környezetek közötti újrafelhasználástól.

3.4 Biztosítani kell a vonatkozó adatvédelmi előírásoknak való megfelelést (pl. GDPR, NIS2) azáltal, hogy minden tesztadat kezelése jogszerűen, tisztességesen és biztonságosan történik.

3.5 A tesztelési gyakorlatok dokumentálásával és egységes védelmi intézkedések alkalmazásával támogatni kell a szervezet külső auditokra és az ISO/IEC 27001 tanúsításra való felkészültségét.

4. Szerepkörök és felelősségek

4.1 Ügyvezető (GM)

4.1.1 Átfogó felelősséggel tartozik a tesztadatok védelméért és a tesztrendszerek biztonságáért.

4.1.2 Jóváhagy minden olyan esetet, amikor valódi adatok tesztelési célú felhasználása történik, miután meggyőződött a megfelelő védelmi intézkedések meglétéről (pl. anonimizálás vagy adatmaszkolás).

4.1.3 Ellenőrzi, hogy a tesztelési tevékenységek megfelelően dokumentáltak és összhangban állnak e szabályzattal.

4.2 Projekttulajdonos

4.2.1 Koordinálja a tesztelési folyamatok kialakítását és végrehajtását.

4.2.2 Biztosítja, hogy minden csapattag megértse és betartsa e szabályzatot.

4.2.3 Megerősíti, hogy a tesztrendszerek a tesztelés megkezdése előtt biztonságosan vannak konfigurálva.

4.2.4 Jelenti az ügyvezetőnek a tesztkörnyezeteket vagy adatszivárgást érintő incidenseket.

[... 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 Ütemezett felülvizsgálatok

9.1.1 Jelen szabályzatot az ügyvezetőnek (GM) legalább évente egyszer felül kell vizsgálnia. A felülvizsgálat biztosítja, hogy a szabályzat naprakész maradjon az alábbiakkal összefüggésben:

9.1.1.1 a szoftverfejlesztési eszközök, platformok vagy környezetek változásai

9.1.1.2 a frissített jogi kötelezettségek, beleértve az adatvédelmi vagy digitális rezilienciára vonatkozó követelményeket

9.1.1.3 a KKV-k ISO/IEC 27001 szerinti tanúsítási és auditfelkészültségi követelményei

9.2 Soron kívüli felülvizsgálatot kiváltó események

9.2.1 További felülvizsgálatot kell végrehajtani az alábbi eseteket követően:

9.2.1.1 bármely incidens, amely a tesztkörnyezetekben adatkitettséggel vagy kompromittálódással jár

9.2.1.2 valódi adatok használata teszteléshez, még akkor is, ha azok anonimizáltak

9.2.1.3 új tesztelési módszerek, rendszerek vagy beszállítók bevezetése

9.2.1.4 olyan szabályozási változások, amelyek érintik az adatok tesztelés során történő kezelését

9.3 Változáskezelés és kommunikáció

9.3.1 Az ügyvezető felelős az alábbiakért:

9.3.1.1 jelen szabályzat frissítése és a módosítások dokumentálása verzióelőzményekkel

9.3.1.2 a munkatársak, fejlesztők és érintett szolgáltatók értesítése a módosításokról

9.3.1.3 annak megerősítése, hogy minden teszteléssel érintett személy megérti és alkalmazza a legfrissebb előírásokat

9.3.1.4 a szabályzat legfrissebb változatának hozzáférhető módon történő fenntartása felülvizsgálati és auditcélokra

9.4 Audit és dokumentáció

9.4.1 A szabályzat valamennyi felülvizsgálatára, a valódi adatok használatának jóváhagyására és minden kivétel indokolására vonatkozó nyilvántartásokat:

9.4.1.1 auditcélból biztonságosan meg kell őrizni

9.4.1.2 kérésre rendelkezésre kell bocsátani belső vagy harmadik fél által végzett audit során

9.4.1.3 évente felül kell vizsgálni a tesztelési gyakorlatokkal való összhang biztosítása érdekében

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzatot az alábbi KKV-szabályzatokkal összehangoltan kell alkalmazni a tesztelés során a biztonság és a megfelelés fenntartása érdekében:

10.1.1 P2S – Irányítási szerepkörök és felelősségek szabályzata: meghatározza, hogy ki felel a fejlesztés, a tesztelés és a rendszerek elkülönítésével kapcsolatos feladatok felügyeletéért.

10.1.2 P4S – Hozzáférés-szabályozási szabályzat: szabályozza a tesztrendszerekhez tartozó hozzáférési hitelesítő adatok kiosztását, kezelését és megszüntetését.

10.1.3 P8S – Információbiztonsági tudatossági és képzési szabályzat: biztosítja, hogy a munkatársak megértsék a tesztadatokhoz kapcsolódó kockázatokat, a biztonságos kezelés gyakorlatát és a környezetek megfelelő elkülönítését.

10.1.4 P13S – Adatosztályozási és címkézési szabályzat: támogatja a tesztadatok egyértelmű osztályozását, valamint iránymutatást ad az anonimizálási és adatmaszkolási stratégiákhoz.

10.1.5 P17S – Adatvédelmi és magánszféra-védelmi szabályzat: összhangot teremt a GDPR-kötelezettségekkel, ideértve a személyes adatok kezelésére és tárolására vonatkozó védelmi intézkedéseket a nem éles környezetekben is.

10.1.6 P24S – Biztonságos fejlesztési szabályzat: átfogó biztonsági elvárásokat határoz meg a fejlesztői csapatok számára, beleértve az adatok tesztelési szakaszokban történő biztonságos használatát is.

10.1.7 P30S – Incidenskezelési szabályzat: meghatározza, hogyan kell reagálni a tesztkörnyezetben észlelt, illetve a tesztadatok nem megfelelő kezeléséből eredő incidensekre.

10.2 Ezek a szabályzatok egységes biztonsági keretrendszert alkotnak a tesztek sértetlenségének, az adattakarékosságnak és a fejlesztési, valamint minőségbiztosítási működés teljes körű ISO/IEC 27001 megfelelőségének támogatására.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 6.1. pont – Előírja a kockázatértékelési és kockázatkezelési intézkedéseket, beleértve a teszteléssel összefüggő kockázatokat is.

11.1.2 8.1. pont – Megköveteli a működési folyamatok tervezését és szabályozását, beleértve a tesztrendszerek kialakítását szolgáló környezeteket is.

11.2 ISO/IEC 27002

11.2.1 8.28. kontroll – Előírja, hogy a szervezetek védjék a tesztadatokat, és biztosítsák, hogy azok ne tartalmazzanak érzékeny vagy éles környezetből származó adatokat.

11.2.2 8.29. kontroll – Megköveteli a fejlesztési, teszt- és éles környezetek egyértelmű elkülönítését.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – A fejlesztésre és tesztelésre vonatkozó kontrollkövetelményeket tartalmazza.

11.3.2 SA-12 – Az ellátási lánchoz kapcsolódó tesztelési kockázatokat és biztonsági értékeléseket kezeli.

11.3.3 SC-32 – Előírja a környezetek elkülönítését, valamint a tesztadatok bizalmasságát és sértetlenségét biztosító védelmet.

11.4 Az Európai Unió általános adatvédelmi rendelete (GDPR)

11.4.1 5. cikk (1) bekezdés c) pont – Előírja az adattakarékosságot, ideértve azt is, hogy teszteléshez csak a szükséges adat használható.

11.4.2 25. cikk – Előírja a beépített és alapértelmezett adatvédelmet, amelybe a tesztkörnyezetek kontrolljai is beletartoznak.

11.4.3 32. cikk – Előírja a személyes adatok biztonságos kezelését valamennyi rendszerben, beleértve a nem éles környezeteket is.

11.5 Az EU NIS2 irányelve (2022/2555)

11.5.1 21. cikk (2) bekezdés e), h) pont – Előírja a biztonságos fejlesztést és a rendszeres tesztelést, különösen ott, ahol a digitális szolgáltatások kiberkockázatnak vannak kitéve.

11.6 Az EU DORA-rendelete (2022/2554)

11.6.1 9. cikk – Hangsúlyozza a digitális működési reziliencia jelentőségét, beleértve az IKT-rendszerek biztonságos tesztelését a pénzügyi szektorban működő KKV-k esetében.

11.7 COBIT 2019

11.7.1 BAI07 – Change Acceptance and Transitioning kezelése: magában foglalja az új rendszerek és adatkezelési gyakorlatok ellenőrzését szolgáló tesztelési kontrollokat.

11.7.2 DSS05 – Biztonsági szolgáltatások kezelése: előírja azokat a tesztelési és fejlesztési gyakorlatokat, amelyek megelőzik az üzleti adatokkal való visszaélést vagy azok kitettségét.