					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P29					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**

A vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	8. fejezet	A tesztadatok és tesztkörnyezetek biztonságos tervezéséhez és szabályozásához kapcsolódik
ISO/IEC 27002:2022	8.28–8.29 kontrollok	A tesztadatok biztonságos kezelésére és a tesztkörnyezetek védelmére terjed ki
NIST SP 800-53 Rev.5	SA-11, SC-28, SC-32	Lefedi a fejlesztői tesztelést és értékelést, a nyugalmi állapotban lévő adatok védelmét, valamint a sértetlenséget
GDPR	5., 25., 32. cikk	Lefedi az adattakarékosságot, a beépített adatvédelmet és az adatkezelés biztonságát tesztelési környezetben
NIS2 irányelv	21. cikk (2) bekezdés e), h) pont	A biztonságos fejlesztési és tesztelési gyakorlatokhoz kapcsolódik
DORA-rendelet	9. cikk	Az IKT-rendszerekhez, protokollokhoz és a tesztadatok biztonságához kapcsolódik
COBIT 2019	DSS05, BAI07	A biztonsági szolgáltatások kezelésére, valamint a változások elfogadására és átvezetésére terjed ki

1. Cél

1.1. Jelen szabályzat meghatározza a tesztkörnyezetek és tesztadatok kezelésére vonatkozó kötelező követelményeket annak érdekében, hogy a szoftverfejlesztési és tesztelési életciklus teljes időtartama alatt biztosított legyen a biztonság, a bizalmasság és a működési sértetlenség.

1.2. A szabályzat célja a jogosulatlan hozzáférés, az adatszivárgás, valamint az éles rendszerek nem megfelelően kezelt tesztkörnyezetből vagy valós adatok tesztelési célú felhasználásából eredő szennyeződésének megelőzése.

1.3. A szabályzat előírja a teszteléshez használt adatok biztonságos kezelését, a tesztinfrastruktúra biztonsági megerősítését és a szerepköralapú hozzáférés-szabályozást, összhangban az alkalmazandó jogszabályi és szerződéses kötelezettségekkel.

2. Hatály

2.1. Jelen szabályzat a szervezet valamennyi, szoftver-, rendszer-, alkalmazás- és infrastruktúra-teszteléshez használt tesztkörnyezetére, adatára, eszközére és folyamatára kiterjed.

2.2. A szabályzat kiterjed különösen az alábbiakra:

2.2.1. helyszíni, felhőalapú vagy harmadik fél platformján létrehozott tesztkörnyezetek

2.2.2. funkcionális, teljesítmény-, regressziós és biztonsági teszteléshez használt tesztadatok

2.2.3. manuális, szkriptalapú vagy automatizált tesztelés, beleértve a CI/CD-folyamatokat

2.2.4. a tesztelésben részt vevő valamennyi munkatárs, beleértve a belső csapatokat, beszállítókat és vállalkozókat

2.3. A szabályzat a rendszerek kritikusságától, az alkalmazás típusától, valamint attól függetlenül alkalmazandó, hogy a fejlesztés belső vagy kiszervezett.

3. Célkitűzések

3.1. Az éles, valós, érzékeny vagy szabályozott adatok (pl. személyazonosításra alkalmas adatok (PII), kártyabirtokosi adatok) tesztkörnyezetben történő használatának megelőzése, kivéve, ha azok anonimizáltak, vagy arra külön jóváhagyás született.

3.2. Annak biztosítása, hogy a teszt- és éles környezetek között teljes hálózati és hozzáférési elkülönítés valósuljon meg a jogosulatlan adathozzáférés vagy a rendszerszennyeződés elkerülése érdekében.

3.3. A titkosítás, az adatmaszkolás vagy a szintetikus adatok előállításának előírása, ha a teszteléshez reprezentatív adatokra van szükség.

3.4. A megfelelőségi hiányosságok, az ügyféladatok kitettsége vagy a nem megfelelően védett tesztadatokból, illetve tesztkörnyezetekből eredő működési zavarok valószínűségének csökkentése.

3.5. A tesztadatok kezelésének összehangolása az iparági szabványokkal (ISO, NIST, COBIT), valamint az olyan szabályozásokkal, mint a GDPR, a NIS2 és a DORA.

4. Szerepkörök és felelősségek

4.1. Információbiztonsági vezető

4.1.1. A szabályzat tulajdonosa, és gondoskodik a tesztadatokra és tesztkörnyezetekre vonatkozó technikai és adminisztratív védelmi intézkedések alkalmazásáról.

4.1.2. Megfelelő indoklás és kompenzáló kontrollok mellett jóváhagyja a valós vagy érzékeny adatok tesztelési célú használatát.

4.2. QA- és tesztvezetők

4.2.1. Koordinálják a tesztelés tervezését, és biztosítják, hogy minden tesztelési tevékenység megfeleljen a jelen szabályzat követelményeinek.

4.2.2. Ellenőrzik a megfelelő elkülönítést, hozzáférést és adat-előkészítést minden tesztelési szakaszban.

[... 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. Jelen szabályzatot évente felül kell vizsgálni, és szükség szerint frissíteni kell az alábbiak figyelembevételével:

9.1.1. a jogszabályi követelmények változásai (pl. GDPR, DORA, NIS2)

9.1.2. új tesztelési eszközök, platformok vagy automatizálási folyamatok bevezetése

9.1.3. belső auditmegállapítások vagy incidens utáni ajánlások

9.1.4. a fejlesztési vagy QA-folyamatok olyan bővülése, amely megváltoztatja a tesztadatok kezelését vagy a tesztkörnyezetek használatát

9.2. A felülvizsgálat kezdeményezéséért az információbiztonsági vezető felel az alábbiakkal együttműködésben:

9.2.1. QA- és tesztvezetők

9.2.2. DevOps- és infrastruktúra-vezetők

9.2.3. alkalmazásfejlesztési csapatok

9.2.4. adatvédelmi tisztviselő és jogi terület

9.3. Valamennyi módosítást:

9.3.1. verziókezeléssel kell ellátni, és a központi dokumentumtárban kell tárolni

9.3.2. formális csatornákon keresztül közölni kell az érintett munkatársakkal (pl. IBIR-értesítések, csapatszintű tájékoztatók)

9.3.3. kapcsolni kell az érintett műszaki szabványok, kontrollok és működési eljárások módosításaihoz

9.4. Eseményvezérelt, soron kívüli felülvizsgálatot kell haladéktalanul végezni az alábbi esetek bármelyikét követően:

9.4.1. tesztkörnyezetet érintő adatszivárgás vagy adatsértés

9.4.2. tesztadat-kezeléssel kapcsolatos auditmegállapításból eredő meg nem felelés

9.4.3. jelentős változás a jogi kötelezettségekben vagy az IT-architektúrában

10. Kapcsolódó szabályzatok és összefüggések

10.1. Jelen szabályzat az alábbi szabályzatokkal szoros összefüggésben alkalmazandó a tesztadatok és tesztkörnyezetek biztonságos és megfelelő kezelésének biztosítása érdekében:

10.1.1. P1 – Információbiztonsági szabályzat: Meghatározza azokat az átfogó biztonsági alapelveket, amelyek a tesztadatok védelmére és a tesztkörnyezetek kezelésére irányadók.

10.1.2. P5 – Változáskezelési szabályzat: Alkalmazandó a tesztkörnyezetek létrehozására, frissítésére és kivonására, valamint a bevezetési folyamatokra.

10.1.3. P13 – Adatosztályozási és címkézési szabályzat: Iránymutatást ad a tesztadatok kiválasztásához és az érzékenységalapú kontrollok alkalmazásához.

10.1.4. P14 – Adatmegőrzési és megsemmisítési szabályzat: Meghatározza a tesztadatkészletek megőrzési időtartamát és a biztonságos megsemmisítés követelményeit.

10.1.5. P15 – Biztonsági mentési és helyreállítási szabályzat: Előírja a biztonsági mentési gyakorlatokat és a helyreállítás ellenőrzését a tesztkörnyezetekre vonatkozóan.

10.1.6. P18 – Kriptográfiai kontrollok szabályzata: Meghatározza a tesztplatformokon nyugalmi állapotban lévő és átvitel alatt álló adatokra vonatkozó kötelező titkosítási szabványokat.

10.1.7. P22 – Naplózási és felügyeleti szabályzat: Szabályozza a tesztkörnyezetekben végzett tevékenységek láthatóságát és a rendellenességek észlelését.

10.1.8. P30 – Incidenskezelési szabályzat: Meghatározza a tesztrendszereket érintő adatsértések vagy incidensek eszkalációját és helyesbítő intézkedéseit.

10.1.9. P33 – Audit- és megfelelőségfelügyeleti szabályzat: Lehetővé teszi a szabályzati megfelelés ellenőrzését és a folyamatos bizonyosság biztosítását.

11. Hivatkozott szabványok és keretrendszerek

11.1. Jelen szabályzat összhangban áll azokkal a globális kiberbiztonsági szabványokkal és szabályozási keretrendszerekkel, amelyek előírják a tesztadatok biztonságos kezelését és a nem éles környezetek védelmét.

11.2. ISO/IEC 27001:

11.2.1. 8.1. pont – Előírja a tesztadatok és tesztkörnyezetek biztonságos tervezését és szabályozását.

11.3. ISO/IEC 27002:2022 – 8.28–8.29 kontrollok:

11.3.1. A melléklet 8.28. kontrollja – Biztonságos tesztadatok: Előírja a fejlesztési és tesztelési szakaszban használt tesztadatok védelmét anonimizálás, adatmaszkolás vagy szintetikus adatok előállítása útján.

11.3.2. A melléklet 8.29. kontrollja – A tesztkörnyezetek védelme: Előírja az éles környezettől való elkülönítést, a hozzáférés-szabályozást és a tesztrendszerek biztonsági megerősítését.

11.3.3. E kontrollok meghatározzák a tesztelés során használt adatok biztonságos kezelésének, valamint a nem éles rendszerek rendeltetésellenes használattal, kompromittálódással vagy szennyeződéssel szembeni védelmének követelményeit.

11.4. NIST SP 800-53 Rev.5:

11.4.1. SA-11 – Fejlesztői tesztelés és értékelés: Meghatározza a biztonságos, ismételhető tesztelési eljárásokra vonatkozó elvárásokat megfelelő adatkontrollok mellett.

11.4.2. SC-28 – A nyugalmi állapotban lévő információk védelme: Összhangban áll a nem éles rendszerekben tárolt tesztadatok titkosításával.

11.4.3. SC-32 – Információs sértetlenség: Támogatja az adatok ellenőrzését, az adatsérülés megelőzését, valamint a be- és kimeneti kontrollokat a tesztelés során.

11.5. GDPR (2016/679):

11.5.1. 5. cikk – Adattakarékosság: Tiltja a személyes adatok indokolatlan használatát tesztelési célra.

11.5.2. 25. cikk – Beépített és alapértelmezett adatvédelem: Előírja, hogy az adatvédelmi technikákat a fejlesztési és tesztelési ciklus kezdetétől alkalmazni kell.

11.5.3. 32. cikk – Az adatkezelés biztonsága: Védelmi intézkedéseket ír elő a személyes vagy érzékeny adatokat kezelő tesztkörnyezetekre.

11.6. NIS2 irányelv (2022/2555):

11.6.1. 21. cikk (2) bekezdés e), h) pont: Előírja a biztonságos szoftverfejlesztési és tesztelési folyamatokat, kiemelve a jogosulatlan hozzáférés és az adatszivárgás elleni védelmet.

11.7. DORA-rendelet (2022/2554):

11.7.1. 9. cikk – IKT-rendszerek és protokollok: Előírja, hogy a tesztelési folyamatok támogassák a rezilienciát, és védjék a működési adatokat a kompromittálódással vagy jogosulatlan közzététellel szemben.

11.8. COBIT 2019:

11.8.1. DSS05 – Biztonsági szolgáltatások kezelése: Támogatja a biztonsági szabályzatok alkalmazását valamennyi környezetben, beleértve a nem éles környezeteket is.

11.8.2. BAI07 – A változások elfogadásának és átvezetésének kezelése: Lefedi a tesztelésből éles környezetbe történő formális átvezetési folyamatot, beleértve az adatokra és környezetekre vonatkozó kontrollokat.