					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P29					Název dokumentu: **Politika testovacích dat a testovacích prostředí**							
Verze: 1.0		Datum účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Standard		Postup		Formulář		Registr		Jiné	

Historie revizí				
Číslo revize	**Datum revize**	**Změny**	**Přezkoumal**	**Vlastník procesu**

Schválení			
Jméno	**Funkce**	**Datum**	**Podpis**

V souladu s normami a právními předpisy

Norma / právní předpis	Kapitola / článek	Komentář
ISO/IEC 27001:2022	Kapitola 8	Relevantní pro bezpečné plánování a řízení testovacích dat a prostředí
ISO/IEC 27002:2022	Opatření 8.28–8.29	Zahrnuje bezpečnost testovacích dat a ochranu testovacích prostředí
NIST SP 800-53 Rev.5	SA-11, SC-28, SC-32	Řeší testování a hodnocení prováděné vývojáři, ochranu dat v klidu a integritu informací
GDPR	Články 5, 25, 32	Zahrnuje minimalizaci údajů, ochranu osobních údajů již od návrhu a zabezpečení zpracování v kontextu testování
směrnice NIS2	Článek 21(2)(e), (h)	Vztahuje se na postupy bezpečného vývoje a testování
nařízení DORA	Článek 9	Týká se systémů a protokolů IKT a bezpečnosti testovacích dat
COBIT 2019	DSS05, BAI07	Zabývá se řízením bezpečnostních služeb a akceptací změn a přechodem do provozu

1. Účel

1.1. Tato politika stanoví závazné požadavky na řízení testovacích prostředí a testovacích dat s cílem zajistit bezpečnost, důvěrnost a provozní integritu v celém životním cyklu vývoje a testování softwaru.

1.2. Jejím cílem je zabránit neoprávněnému přístupu, úniku dat a kontaminaci produkčních systémů v důsledku nedostatečně řízených testovacích prostředí nebo používání reálných dat při testování.

1.3. Tato politika vyžaduje bezpečné nakládání s daty používanými pro testování, hardening testovací infrastruktury a řízení přístupu na základě rolí, a je v souladu s příslušnými regulatorními požadavky a smluvními povinnostmi.

2. Rozsah

2.1. Tato politika se vztahuje na všechna testovací prostředí, data, nástroje a procesy používané pro testování softwaru, systémů, aplikací a infrastruktury v celé organizaci.

2.2. Zahrnuje:

2.2.1. testovací prostředí zřízená on-premises, v cloudu nebo prostřednictvím platforem třetích stran

2.2.2. testovací data používaná při funkčním, výkonnostním, regresním a bezpečnostním testování

2.2.3. manuální, skriptované nebo automatizované testování (např. CI/CD pipeline)

2.2.4. veškerý personál zapojený do testování, včetně interních týmů, dodavatelů a smluvních pracovníků

2.3. Tato politika se uplatňuje bez ohledu na kritičnost systému, typ aplikace nebo na to, zda je vývoj interní nebo outsourcovaný.

3. Cíle

3.1. Zabránit používání produkčních, citlivých nebo regulovaných dat (např. osobně identifikovatelných údajů (PII), údajů držitelů platebních karet) v testovacích prostředích, pokud nejsou anonymizována nebo výslovně schválena.

3.2. Zajistit úplné síťové a přístupové oddělení mezi testovacími a produkčními prostředími, aby se zabránilo neoprávněnému přístupu k datům nebo kontaminaci systémů.

3.3. Vyžadovat šifrování, maskování dat nebo generování syntetických dat, pokud jsou pro účely testování nezbytná reprezentativní data.

3.4. Snížit pravděpodobnost nesouladu, expozice zákaznických dat nebo narušení provozu vyplývajících z nedostatečně zabezpečených testovacích dat nebo prostředí.

3.5. Uvést nakládání s testovacími daty do souladu s oborově uznávanými normami (ISO, NIST, COBIT) a předpisy, jako jsou GDPR, NIS2 a DORA.

4. Role a odpovědnosti

4.1. Ředitel informační bezpečnosti (CISO)

4.1.1. Je vlastníkem této politiky a prosazuje technická a administrativní bezpečnostní opatření pro testovací data a prostředí.

4.1.2. Schvaluje použití reálných nebo citlivých dat při testování na základě odpovídajícího odůvodnění a při zavedení kompenzačních opatření.

4.2. Vedoucí QA/testování

4.2.1. Koordinují plánování testování a zajišťují, aby všechny testovací činnosti byly v souladu s požadavky této politiky.

4.2.2. Ověřují odpovídající oddělení prostředí, nastavení přístupu a přípravu dat pro každou fázi testování.

[... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ...]

9. Požadavky na přezkoumávání a aktualizaci

9.1. Tato politika musí být přezkoumávána každoročně a podle potřeby aktualizována tak, aby odrážela:

9.1.1. změny regulatorních požadavků (např. GDPR, DORA, NIS2)

9.1.2. zavedení nových testovacích nástrojů, platforem nebo automatizačních pipeline

9.1.3. zjištění interního auditu nebo doporučení z přezkoumání po incidentu

9.1.4. rozšíření vývojových nebo QA procesů, která mění nakládání s testovacími daty nebo používání prostředí

9.2. CISO odpovídá za zahájení přezkumu ve spolupráci s:

9.2.1. vedoucími QA/testování

9.2.2. manažery DevOps a infrastruktury

9.2.3. týmy aplikačního vývoje

9.2.4. pověřencem pro ochranu osobních údajů a právním oddělením

9.3. Všechny revize musí být:

9.3.1. vedeny v režimu správy verzí a uloženy v centrálním repozitáři dokumentů

9.3.2. komunikovány dotčenému personálu prostřednictvím formálních kanálů (např. oznámení ISMS, týmové briefingy)

9.3.3. propojeny s aktualizacemi souvisejících technických standardů, opatření a provozních postupů

9.4. Mimořádné přezkumy vyvolané událostí musí být provedeny bezodkladně po jakémkoli:

9.4.1. úniku dat nebo porušení zabezpečení dat týkajícím se testovacích prostředí

9.4.2. zjištění neshody z auditu související s nakládáním s testovacími daty

9.4.3. významné změně právních povinností nebo IT architektury

10. Související politiky a vazby

10.1. Tato politika je úzce propojena s následujícími politikami, aby bylo zajištěno bezpečné nakládání s testovacími daty a prostředími v souladu s požadavky:

10.1.1. P1 – Politika informační bezpečnosti: Stanoví zastřešující principy bezpečnosti, kterými se řídí ochrana testovacích dat a správa prostředí.

10.1.2. P5 – Politika řízení změn: Vztahuje se na vytváření, aktualizaci a vyřazování testovacích prostředí a nasazovacích pipeline.

10.1.3. P13 – Politika klasifikace dat a označování: Určuje výběr testovacích dat a uplatňování opatření podle citlivosti.

10.1.4. P14 – Politika uchovávání údajů: Stanoví retenční lhůty a požadavky na bezpečnou likvidaci testovacích datových sad.

10.1.5. P15 – Politika zálohování a obnovy: Vyžaduje postupy zálohování a ověření obnovy pro testovací prostředí.

10.1.6. P18 – Politika kryptografických opatření: Stanoví závazné standardy šifrování pro data v klidu a data při přenosu v rámci testovacích platforem.

10.1.7. P22 – Politika protokolování a monitorování: Upravuje viditelnost a detekci anomálií v aktivitách testovacích prostředí.

10.1.8. P30 – Politika reakce na incidenty: Definuje eskalaci a nápravná opatření pro porušení zabezpečení dat nebo incidenty týkající se testovacích systémů.

10.1.9. P33 – Politika monitorování auditu a souladu: Umožňuje ověřování dodržování politiky a průběžné zajištění souladu.

11. Referenční normy a rámce

11.1. Tato politika je v souladu s globálními normami kybernetické bezpečnosti a regulatorními rámci, které vyžadují bezpečné nakládání s testovacími daty a ochranu neprodukčních prostředí.

11.2. ISO/IEC 27001:

11.2.1. Kapitola 8.1 – Vyžaduje bezpečné plánování a řízení testovacích dat a prostředí.

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

11.3.1. Příloha A, Opatření 8.28 – Bezpečná testovací data: Vyžaduje ochranu testovacích dat používaných ve fázích vývoje a testování prostřednictvím anonymizace, maskování dat nebo syntetického generování.

11.3.2. Příloha A, Opatření 8.29 – Ochrana testovacích prostředí: Vyžaduje oddělení od produkce, řízení přístupu a hardening prostředí pro testovací systémy.

11.3.3. Tato opatření stanoví požadavky na bezpečné řízení dat používaných během testování a na ochranu neprodukčních systémů před zneužitím, kompromitací nebo kontaminací.

11.4. NIST SP 800-53 Rev.5:

11.4.1. SA-11 – Testování a hodnocení prováděné vývojáři: Stanoví očekávání pro bezpečné a opakovatelné postupy testování s odpovídajícími opatřeními pro data.

11.4.2. SC-28 – Ochrana informací v klidu: Je v souladu se šifrováním testovacích dat uložených v neprodukčních systémech.

11.4.3. SC-32 – Integrita informací: Podporuje ověřování dat, prevenci poškození a řízení vstupů a výstupů během testování.

11.5. GDPR (2016/679):

11.5.1. Článek 5 – Minimalizace údajů: Zakazuje zbytečné používání osobních údajů při testování.

11.5.2. Článek 25 – Ochrana osobních údajů již od návrhu: Vyžaduje uplatnění technik ochrany údajů od počátku cyklu vývoje a testování.

11.5.3. Článek 32 – Zabezpečení zpracování: Vyžaduje bezpečnostní opatření pro testovací prostředí, která nakládají s osobními nebo citlivými údaji.

11.6. směrnice NIS2 (2022/2555):

11.6.1. Článek 21(2)(e, h): Vyžaduje bezpečné procesy vývoje a testování softwaru s důrazem na ochranu před neoprávněným přístupem a únikem dat.

11.7. nařízení DORA (2022/2554):

11.7.1. Článek 9 – Systémy a protokoly IKT: Vyžaduje, aby testovací procesy podporovaly odolnost a chránily provozní data před kompromitací nebo neoprávněným zpřístupněním.

11.8. COBIT 2019:

11.8.1. DSS05 – Řízení bezpečnostních služeb: Podporuje prosazování bezpečnostních politik ve všech prostředích, včetně neprodukčních.

11.8.2. BAI07 – Řízení akceptace změn a přechodu: Zahrnuje formální proces přechodu z testování do produkce, včetně opatření pro data a prostředí.