					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P29					Názov dokumentu: **Politika testovacích údajov a testovacieho prostredia – SME**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Štandard		Postup		Formulár		Register		Iné	

História revízií				
Číslo revízie	**Dátum revízie**	**Zmeny**	**Preskúmal**	**Vlastník procesu**

Schválenia			
Meno	**Pozícia**	**Dátum**	**Podpis**

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitola 8	Relevantné pre bezpečné plánovanie a riadenie testovacích údajov a prostredí
ISO/IEC 27002:2022	Kontroly 8.28–8.29	Zahŕňa bezpečné testovacie údaje a ochranu testovacích prostredí
NIST SP 800-53 Rev.5	SA-11, SC-28, SC-32	Rieši testovanie a hodnotenie vývojárov, ochranu údajov v pokoji a integritu
Nariadenie EÚ GDPR	Články 5, 25, 32	Zahŕňa minimalizáciu údajov, ochranu súkromia už od návrhu a bezpečnosť spracúvania v kontexte testovania
Smernica EÚ NIS2	Článok 21(2)(e), (h)	Súvisí s bezpečnými postupmi vývoja a testovania
Nariadenie EÚ DORA	Článok 9	Týka sa systémov IKT, protokolov a bezpečnosti testovacích údajov
COBIT 2019	DSS05, BAI07	Zaoberá sa riadením bezpečnostných služieb a akceptáciou zmien a prechodom do prevádzky

1. Účel

1.1. Táto politika stanovuje záväzné požiadavky na riadenie testovacích prostredí a testovacích údajov s cieľom zabezpečiť bezpečnosť, dôvernosť a prevádzkovú integritu počas celého životného cyklu vývoja softvéru a testovania.

1.2. Jej cieľom je predchádzať neoprávnenému prístupu, únikom údajov a kontaminácii produkčných systémov v dôsledku nedostatočne riadených testovacích prostredí alebo používania reálnych údajov pri testovaní.

1.3. Táto politika vyžaduje bezpečné nakladanie s údajmi používanými na testovanie, bezpečné spevnenie testovacej infraštruktúry a riadenie prístupu na základe rolí (RBAC), pričom je v súlade s uplatniteľnými zákonnými, regulačnými a zmluvnými povinnosťami.

2. Rozsah

2.1. Táto politika sa vzťahuje na všetky testovacie prostredia, údaje, nástroje a procesy používané na testovanie softvéru, systémov, aplikácií a infraštruktúry v celej organizácii.

2.2. Zahŕňa:

2.2.1. Testovacie prostredia zriadené vo vlastných priestoroch, v cloudovom prostredí alebo prostredníctvom platforiem tretích strán

2.2.2. Testovacie údaje používané pri funkčnom, výkonnostnom, regresnom a bezpečnostnom testovaní

2.2.3. Manuálne, skriptované alebo automatizované testovanie (napr. CI/CD pipeline)

2.2.4. Všetkých pracovníkov zapojených do testovania vrátane interných tímov, dodávateľov a zmluvných pracovníkov

2.3. Táto politika sa uplatňuje bez ohľadu na kritickosť systému, typ aplikácie alebo to, či je vývoj interný alebo outsourcovaný.

3. Ciele

3.1. Zabrániť používaniu prevádzkových, citlivých alebo regulovaných údajov (napr. osobne identifikovateľné údaje (PII), údaje o platobných kartách) v testovacích prostrediach, pokiaľ nie sú anonymizované alebo osobitne schválené.

3.2. Zabezpečiť úplnú sieťovú a prístupovú segregáciu medzi testovacími a produkčnými prostrediami, aby sa predišlo neoprávnenému prístupu k údajom alebo kontaminácii systémov.

3.3. Vyžadovať šifrovanie, maskovanie údajov alebo generovanie syntetických údajov, ak sú na účely testovania potrebné reprezentatívne údaje.

3.4. Znížiť pravdepodobnosť zlyhaní v oblasti súladu, vystavenia údajov zákazníkov alebo prevádzkových narušení vyplývajúcich z nezabezpečených testovacích údajov alebo prostredí.

3.5. Zosúladiť nakladanie s testovacími údajmi s osvedčenými postupmi a normami odvetvia (ISO, NIST, COBIT) a s predpismi, ako sú GDPR, NIS2 a DORA.

4. Roly a zodpovednosti

4.1. Riaditeľ informačnej bezpečnosti (CISO)

4.1.1. Je vlastníkom tejto politiky a zabezpečuje technické a administratívne ochranné opatrenia pre testovacie údaje a testovacie prostredia.

4.1.2. Schvaľuje používanie reálnych alebo citlivých údajov pri testovaní na základe primeraného odôvodnenia a pri zavedení kompenzačných kontrol.

4.2. Vedúci kvality a testovania

4.2.1. Koordinujú plánovanie testovania a zabezpečujú, aby všetky testovacie činnosti boli v súlade s požiadavkami tejto politiky.

4.2.2. Overujú primeranú segregáciu, prístup a prípravu údajov pre každú fázu testovania.

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Požiadavky na preskúmanie a aktualizáciu

9.1. Táto politika sa musí preskúmavať každoročne a podľa potreby aktualizovať tak, aby odrážala:

9.1.1. Zmeny regulačných požiadaviek (napr. GDPR, DORA, NIS2)

9.1.2. Zavedenie nových testovacích nástrojov, platforiem alebo automatizačných pipeline

9.1.3. Auditné zistenia interného auditu alebo odporúčania z poincidentných revízií

9.1.4. Rozšírenie vývojových alebo testovacích procesov kvality, ktoré menia nakladanie s testovacími údajmi alebo používanie prostredí

9.2. CISO zodpovedá za iniciovanie preskúmania v spolupráci s:

9.2.1. Vedúcimi kvality a testovania

9.2.2. Manažérmi DevOps a infraštruktúry

9.2.3. Tímami vývoja aplikácií

9.2.4. Zodpovednou osobou pre ochranu osobných údajov a právnym oddelením

9.3. Všetky revízie musia byť:

9.3.1. Riadené verziami a uložené v centrálnom úložisku dokumentov

9.3.2. Oznámené dotknutým pracovníkom prostredníctvom formálnych kanálov (napr. notifikácie ISMS, tímové poučenia)

9.3.3. Prepojené s aktualizáciami súvisiacich technických štandardov, kontrol a prevádzkových postupov

9.4. Medziobdobné preskúmania na základe spúšťacej udalosti sa musia vykonať bezodkladne po každom:

9.4.1. Úniku údajov alebo porušení ochrany údajov v testovacích prostrediach

9.4.2. Nezhodnom auditnom zistení súvisiacom s nakladaním s testovacími údajmi

9.4.3. Významnej zmene zákonných povinností alebo IT architektúry

10. Súvisiace politiky a väzby

10.1. Táto politika je úzko prepojená s nasledujúcimi politikami s cieľom zabezpečiť bezpečné nakladanie s testovacími údajmi a testovacími prostrediami v súlade s požiadavkami:

10.1.1. P1 – Politika informačnej bezpečnosti: stanovuje nadradené princípy bezpečnosti, ktoré upravujú ochranu testovacích údajov a riadenie prostredí.

10.1.2. P5 – Politika riadenia zmien: vzťahuje sa na vytváranie, aktualizáciu a vyradenie testovacích prostredí a nasadzovacích pipeline.

10.1.3. P13 – Politika klasifikácie a označovania údajov: usmerňuje výber testovacích údajov a uplatňovanie kontrol podľa citlivosti.

10.1.4. P14 – Politika uchovávania a likvidácie údajov: určuje lehoty uchovávania a požiadavky na bezpečnú likvidáciu testovacích súborov údajov.

10.1.5. P15 – Politika zálohovania a obnovy: stanovuje požiadavky na zálohovanie a validáciu obnovy pre testovacie prostredia.

10.1.6. P18 – Politika kryptografických kontrol: špecifikuje záväzné štandardy šifrovania pre údaje v pokoji a pri prenose v rámci testovacích platforiem.

10.1.7. P22 – Politika logovania a monitorovania: upravuje viditeľnosť a detekciu anomálií pri aktivitách v testovacích prostrediach.

10.1.8. P30 – Politika reakcie na incidenty: definuje eskaláciu a nápravné opatrenia pri porušeniach ochrany údajov alebo incidentoch týkajúcich sa testovacích systémov.

10.1.9. P33 – Politika monitorovania auditu a súladu: umožňuje overovanie dodržiavania politiky a priebežné uisťovanie.

11. Referenčné normy a rámce

11.1. Táto politika je zosúladená s globálnymi normami kybernetickej bezpečnosti a regulačnými rámcami, ktoré vyžadujú bezpečné nakladanie s testovacími údajmi a ochranu neprodukčných prostredí.

11.2. ISO/IEC 27001:

11.2.1. Kapitola 8.1 – vyžaduje bezpečné plánovanie a riadenie testovacích údajov a prostredí.

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

11.3.1. Príloha A, kontrola 8.28 – Bezpečné testovacie údaje: vyžaduje ochranu testovacích údajov používaných vo vývojových a testovacích fázach prostredníctvom anonymizácie, maskovania alebo generovania syntetických údajov.

11.3.2. Príloha A, kontrola 8.29 – Ochrana testovacích prostredí: vyžaduje segregáciu od produkcie, riadenie prístupu a spevnenie konfigurácie testovacích prostredí.

11.3.3. Tieto kontroly stanovujú požiadavky na bezpečné riadenie údajov používaných počas testovania a na ochranu neprodukčných systémov pred zneužitím, kompromitáciou alebo kontamináciou.

11.4. NIST SP 800-53 Rev.5:

11.4.1. SA-11 – Testovanie a hodnotenie vývojárov: stanovuje očakávania na bezpečné a opakovateľné postupy testovania s primeranými kontrolami údajov.

11.4.2. SC-28 – Ochrana informácií v pokoji: je v súlade so šifrovaním testovacích údajov uložených v neprodukčných systémoch.

11.4.3. SC-32 – Integrita informácií: podporuje validáciu údajov, prevenciu poškodenia a kontroly vstupov a výstupov počas testovania.

11.5. Nariadenie EÚ GDPR (2016/679):

11.5.1. Článok 5 – Minimalizácia údajov: zakazuje zbytočné používanie osobných údajov pri testovaní.

11.5.2. Článok 25 – Ochrana súkromia už od návrhu: vyžaduje, aby sa techniky ochrany údajov uplatňovali od začiatku vývojového a testovacieho cyklu.

11.5.3. Článok 32 – Bezpečnosť spracúvania: vyžaduje ochranné opatrenia pre testovacie prostredia, ktoré spracúvajú osobné alebo citlivé údaje.

11.6. Smernica EÚ NIS2 (2022/2555):

11.6.1. Článok 21(2)(e), (h): vyžaduje bezpečné procesy vývoja softvéru a testovania s dôrazom na ochranu pred neoprávneným prístupom a únikom údajov.

11.7. Nariadenie EÚ DORA (2022/2554):

11.7.1. Článok 9 – Systémy IKT a protokoly: vyžaduje, aby testovacie procesy podporovali odolnosť a chránili prevádzkové údaje pred kompromitáciou alebo neoprávneným sprístupnením.

11.8. COBIT 2019:

11.8.1. DSS05 – Riadenie bezpečnostných služieb: podporuje uplatňovanie bezpečnostných politík vo všetkých prostrediach vrátane neprodukčných.

11.8.2. BAI07 – Riadenie akceptácie zmien a prechodu: zahŕňa formálny proces prechodu z testovania do produkcie vrátane kontrol údajov a prostredí.