					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P29S					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**

Zosúladenie s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitoly 6.1, 8	
ISO/IEC 27002:2022	Kontroly 8.28–8.29	
NIST SP 800-53 Rev. 5	SA-11, SA-12, SC-32	
Nariadenie EÚ GDPR	Články 5 ods. 1 písm. c), 25, 32	
Smernica EÚ NIS2	Článok 21 ods. 2 písm. e), h)	
Nariadenie EÚ DORA	Článok 9	
COBIT 2019	BAI07, DSS05	

1. Účel

1.1 Táto politika stanovuje spôsob správy testovacích údajov a testovacích prostredí tak, aby sa predišlo náhodnému sprístupneniu údajov, narušeniu ochrany údajov alebo prevádzkovým výpadkom počas testovacích činností.

1.2 Zabezpečuje, aby sa pri testovaní softvéru alebo systémov nepoužívali skutočné údaje zákazníkov neprimeraným spôsobom a aby boli testovacie prostredia logicky aj technicky oddelené od produkčných systémov.

1.3 Táto politika je určená na podporu malých a stredných podnikov pri plnení požiadaviek certifikácie podľa ISO/IEC 27001 a príslušných právnych predpisov v oblasti ochrany údajov, pričom zostáva praktická a uplatniteľná aj pre organizácie bez vyhradeného IT tímu.

2. Rozsah

2.1 Táto politika sa vzťahuje na:

2.1.1 všetky testovacie prostredia (napr. staging servery, sandbox prostredia, vývojové testovacie prostredia)

2.1.2 všetky testovacie údaje bez ohľadu na to, či boli vytvorené manuálne, generované alebo odvodené z produkčných údajov

2.1.3 všetky osoby zapojené do testovacích činností vrátane zamestnancov, zmluvných pracovníkov, freelancerov a poskytovateľov IT služieb

2.1.4 akékoľvek testovanie, ktoré môže mať vplyv na platformy dostupné zákazníkom, interné podnikové systémy alebo služby tretích strán

2.2 Zahŕňa technické prostredia aj procesy používané na podporu:

2.2.1 vývoja webových sídiel, aplikácií a nástrojov

2.2.2 aktualizácií systémov, testovania konfigurácie a integračného testovania

2.2.3 automatizovaného a manuálneho funkčného alebo bezpečnostného testovania

3. Ciele

3.1 Zabrániť používaniu skutočných identifikovateľných údajov zákazníkov pri testovaní, pokiaľ nie sú anonymizované a výslovne schválené.

3.2 Zachovať prísne oddelenie testovacích a produkčných systémov s cieľom predchádzať nechcenému sprístupneniu údajov alebo zásahom do prevádzky.

3.3 Chrániť testovacie systémy a údaje pred neoprávneným prístupom, náhodným sprístupnením alebo opätovným použitím medzi prostrediami bez primeraných kontrol.

3.4 Zabezpečiť súlad s príslušnými predpismi na ochranu údajov (napr. GDPR, NIS2) tak, aby sa všetky testovacie údaje spracúvali zákonne, spravodlivo a bezpečne.

3.5 Podporiť pripravenosť organizácie na externé audity a certifikáciu podľa ISO/IEC 27001 prostredníctvom dokumentovania testovacích postupov a uplatňovania konzistentných ochranných opatrení.

4. Roly a zodpovednosti

4.1 Generálny manažér (GM)

4.1.1 Nesie celkovú zodpovednosť za ochranu testovacích údajov a bezpečnosť testovacích systémov.

4.1.2 Schvaľuje akékoľvek použitie skutočných údajov pri testovaní po overení primeraných ochranných opatrení (napr. anonymizácie alebo maskovania).

4.1.3 Overuje, že testovacie činnosti sú riadne zdokumentované a vykonávajú sa v súlade s touto politikou.

4.2 Vlastník projektu

4.2.1 Koordinuje návrh a realizáciu testovacích procesov.

4.2.2 Zabezpečuje, aby všetci členovia tímu tejto politike rozumeli a dodržiavali ju.

4.2.3 Potvrdzuje, že testovacie systémy sú pred začatím testovania bezpečne nakonfigurované.

4.2.4 Oznamuje GM všetky incidenty týkajúce sa testovacích prostredí alebo únikov údajov.

[... 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 Plánované preskúmania

9.1.1 Túto politiku musí minimálne raz ročne preskúmať generálny manažér (GM). Preskúmanie zabezpečuje, že politika zostáva aktuálna vzhľadom na:

9.1.1.1 zmeny vo vývojových nástrojoch, platformách alebo prostrediach

9.1.1.2 aktualizované právne povinnosti vrátane požiadaviek na ochranu údajov alebo digitálnu prevádzkovú odolnosť

9.1.1.3 certifikáciu malých a stredných podnikov a pripravenosť na audit podľa ISO/IEC 27001

9.2 Spúšťacie udalosti priebežného preskúmania

9.2.1 Dodatočné preskúmania sa musia vykonať po:

9.2.1.1 akomkoľvek incidente zahŕňajúcom sprístupnenie údajov alebo kompromitáciu v testovacích prostrediach

9.2.1.2 použití skutočných údajov pri testovaní, aj keď sú anonymizované

9.2.1.3 zavedení nových metód testovania, systémov alebo dodávateľov

9.2.1.4 regulačných zmenách ovplyvňujúcich spôsob nakladania s údajmi počas testovania

9.3 Riadenie zmien a komunikácia

9.3.1 GM zodpovedá za:

9.3.1.1 aktualizáciu tejto politiky a zdokumentovanie všetkých revízií v histórii verzií

9.3.1.2 informovanie zamestnancov, vývojárov a príslušných poskytovateľov služieb o aktualizáciách

9.3.1.3 potvrdenie, že všetci pracovníci zapojení do testovania rozumejú najnovším pravidlám a uplatňujú ich

9.3.1.4 udržiavanie prístupnej verzie aktuálnej politiky na účely preskúmania a auditu

9.4 Audit a dokumentácia

9.4.1 Záznamy o všetkých preskúmaniach politiky, schváleniach použitia skutočných údajov a odôvodneniach výnimiek musia byť:

9.4.1.1 bezpečne uchovávané na účely auditu

9.4.1.2 dostupné na požiadanie počas interných auditov alebo auditov tretích strán

9.4.1.3 každoročne preskúmavané s cieľom zabezpečiť súlad s testovacími postupmi

10. Súvisiace politiky a väzby

10.1 Táto politika sa musí uplatňovať v koordinácii s nasledujúcimi SME politikami s cieľom zachovať bezpečnosť a súlad počas testovania:

10.1.1 P2S – Politika rolí a zodpovedností v riadení: Definuje, kto nesie zodpovednosť za dohľad nad vývojom, testovaním a povinnosťami pri oddelení systémov.

10.1.2 P4S – Politika riadenia prístupu: Upravuje prideľovanie, správu a odoberanie prístupových údajov do testovacích systémov.

10.1.3 P8S – Politika zvyšovania povedomia o informačnej bezpečnosti a školení: Zabezpečuje, aby pracovníci rozumeli rizikám testovacích údajov, postupom bezpečného nakladania a správnemu oddeleniu prostredí.

10.1.4 P13S – Politika klasifikácie a označovania údajov: Podporuje jednoznačnú klasifikáciu testovacích údajov a usmerňuje stratégie anonymizácie alebo maskovania.

10.1.5 P17S – Politika ochrany údajov a súkromia: Je zosúladená s povinnosťami podľa GDPR vrátane ochranných opatrení pri spracúvaní a ukladaní osobných údajov aj v testovacích prostrediach.

10.1.6 P24S – Politika bezpečného vývoja: Stanovuje celkové bezpečnostné očakávania pre vývojové tímy vrátane bezpečného používania údajov počas fáz testovania.

10.1.7 P30S – Politika reakcie na incidenty: Určuje, ako reagovať na akékoľvek narušenie alebo problém zistený v testovacom prostredí alebo spôsobený nesprávnym nakladaním s testovacími údajmi.

10.2 Tieto politiky tvoria jednotný rámec informačnej bezpečnosti na podporu integrity testovania, minimalizácie údajov a úplného súladu s ISO/IEC 27001 v rámci vývojových činností a zabezpečenia kvality.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 6.1 – Vyžaduje posúdenie rizík a opatrenia na ich ošetrenie vrátane rizík súvisiacich s testovaním.

11.1.2 Kapitola 8.1 – Vyžaduje plánovanie a riadenie prevádzkových procesov vrátane zriadenia prostredí testovacích systémov.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.28 – Vyžaduje, aby organizácie chránili testovacie údaje a zabezpečili, že neobsahujú citlivé údaje ani produkčné údaje.

11.2.2 Kontrola 8.29 – Vyžaduje jednoznačné oddelenie vývojových, testovacích a produkčných prostredí.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-11 – Zahŕňa požiadavky na kontroly vo vývoji a testovaní.

11.3.2 SA-12 – Rieši riziká testovania v dodávateľskom reťazci a bezpečnostné hodnotenia.

11.3.3 SC-32 – Vyžaduje oddelenie prostredí a ochranu dôvernosti a integrity testovacích údajov.

11.4 Všeobecné nariadenie EÚ o ochrane údajov (GDPR)

11.4.1 Článok 5 ods. 1 písm. c) – Vyžaduje minimalizáciu údajov vrátane používania iba nevyhnutných údajov na testovanie.

11.4.2 Článok 25 – Vyžaduje ochranu údajov už v štádiu návrhu, čo zahŕňa aj kontroly testovacích prostredí.

11.4.3 Článok 32 – Vyžaduje bezpečné spracúvanie osobných údajov vo všetkých systémoch vrátane neprodukčných prostredí.

11.5 Smernica EÚ NIS2 (2022/2555)

11.5.1 Článok 21 ods. 2 písm. e), h) – Vyžaduje bezpečný vývoj a testovanie systémov, najmä tam, kde sú digitálne služby vystavené kybernetickému riziku.

11.6 Nariadenie EÚ DORA (2022/2554)

11.6.1 Článok 9 – Zdôrazňuje význam digitálnej prevádzkovej odolnosti vrátane bezpečného testovania IKT systémov v malých a stredných podnikoch vo finančnom sektore.

11.7 COBIT 2019

11.7.1 BAI07 – Riadenie akceptácie zmien a prechodu do prevádzky: Zahŕňa testovacie kontroly na overenie nových systémov a nakladania s údajmi.

11.7.2 DSS05 – Riadenie bezpečnostných služieb: Vyžaduje testovacie a vývojové postupy, ktoré zabraňujú zneužitiu alebo sprístupneniu informácií organizácie.