					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P29S					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	Kapitoly 6.1, 8	
ISO/IEC 27002:2022	Opatření 8.28–8.29	
NIST SP 800-53 Rev. 5	SA-11, SA-12, SC-32	
GDPR	Články 5 odst. 1 písm. c), 25, 32	
směrnice NIS2	Článek 21 odst. 2 písm. e), h)	
nařízení DORA	Článek 9	
COBIT 2019	BAI07, DSS05	

1. Účel

1.1 Tato politika stanoví, jak musí být řízena testovací data a testovací prostředí, aby se při testovacích činnostech předešlo náhodnému zpřístupnění dat, narušení bezpečnosti dat nebo provozním výpadkům.

1.2 Zajišťuje, že skutečná zákaznická data nebudou při testování softwaru nebo systémů nikdy použita nevhodným způsobem a že testovací prostředí budou logicky i technicky oddělena od produkčních systémů.

1.3 Tato politika je navržena tak, aby pomáhala SME plnit požadavky na certifikaci podle ISO/IEC 27001 a příslušné právní předpisy v oblasti ochrany osobních údajů, a zároveň byla praktická a vymahatelná i pro organizace bez vyhrazeného IT týmu.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 všechna testovací prostředí (např. staging servery, sandboxy, vývojové testovací platformy),

2.1.2 veškerá testovací data, ať už ručně vytvořená, generovaná nebo odvozená z provozních dat,

2.1.3 veškerý personál zapojený do testovacích činností, včetně zaměstnanců, dodavatelů, freelancerů a poskytovatelů IT služeb,

2.1.4 jakékoli testování, které by mohlo ovlivnit zákaznické platformy, interní podnikové systémy nebo služby třetích stran.

2.2 Pokrývá technická prostředí i procesy používané na podporu:

2.2.1 vývoje webových stránek, aplikací a nástrojů,

2.2.2 modernizace systémů, testování konfigurací a integračního testování,

2.2.3 automatizovaného i manuálního funkčního nebo bezpečnostního testování.

3. Cíle

3.1 Zabránit použití skutečných identifikovatelných zákaznických dat při testování, pokud nejsou anonymizována a výslovně schválena.

3.2 Udržovat přísné oddělení mezi testovacími a produkčními systémy, aby se předešlo neúmyslnému zpřístupnění dat nebo provoznímu ovlivnění.

3.3 Chránit testovací systémy a data před neoprávněným přístupem, náhodným zpřístupněním nebo opětovným použitím napříč prostředími bez odpovídajících opatření.

3.4 Zajistit soulad s příslušnými předpisy na ochranu osobních údajů (např. GDPR, směrnice NIS2) tím, že veškerá testovací data budou zpracovávána zákonným, korektním a bezpečným způsobem.

3.5 Podpořit připravenost organizace na externí audity a certifikaci podle ISO/IEC 27001 dokumentováním testovacích postupů a uplatňováním konzistentních ochranných opatření.

4. Role a odpovědnosti

4.1 generální ředitel (GM)

4.1.1 Nese celkovou odpovědnost za ochranu testovacích dat a zabezpečení testovacích systémů.

4.1.2 Schvaluje jakékoli použití skutečných dat při testování po ověření, že jsou zavedena odpovídající ochranná opatření (např. anonymizace nebo maskování dat).

4.1.3 Ověřuje, že testovací činnosti jsou řádně dokumentovány a v souladu s touto politikou.

4.2 vlastník projektu

4.2.1 Koordinuje návrh a provádění testovacích procesů.

4.2.2 Zajišťuje, aby všichni členové týmu této politice rozuměli a dodržovali ji.

4.2.3 Potvrzuje, že testovací systémy jsou před zahájením testování bezpečně nakonfigurovány.

4.2.4 Hlášení incidentů týkajících se testovacích prostředí nebo úniků dat předává GM.

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

9. Požadavky na přezkoumávání a aktualizaci

9.1 Plánované přezkumy

9.1.1 Tato politika musí být nejméně jednou ročně přezkoumána generálním ředitelem (GM). Přezkum zajišťuje, že politika zůstává aktuální s ohledem na:

9.1.1.1 změny nástrojů, platforem nebo prostředí pro vývoj softwaru,

9.1.1.2 aktualizované právní povinnosti, včetně požadavků na ochranu osobních údajů nebo digitální provozní odolnost,

9.1.1.3 připravenost SME na certifikaci a audit podle ISO/IEC 27001.

9.2 Spouštěcí události pro mimořádný přezkum

9.2.1 Další přezkumy musí proběhnout po:

9.2.1.1 jakémkoli incidentu zahrnujícím zpřístupnění dat nebo kompromitaci v testovacích prostředích,

9.2.1.2 použití skutečných dat při testování, i pokud byla anonymizována,

9.2.1.3 zavedení nových testovacích metod, systémů nebo dodavatelů,

9.2.1.4 regulatorních změnách ovlivňujících nakládání s daty během testování.

9.3 Řízení změn a komunikace

9.3.1 GM odpovídá za:

9.3.1.1 aktualizaci této politiky a dokumentování všech změn v historii verzí,

9.3.1.2 informování zaměstnanců, vývojářů a příslušných poskytovatelů služeb o aktualizacích,

9.3.1.3 potvrzení, že veškerý personál související s testováním rozumí aktuálním pravidlům a uplatňuje je,

9.3.1.4 udržování přístupné aktuální verze politiky pro účely přezkumu a auditu.

9.4 Audit a dokumentace

9.4.1 Záznamy o všech přezkumech politiky, schváleních použití skutečných dat a odůvodněních výjimek musí být:

9.4.1.1 bezpečně uchovávány pro účely auditu,

9.4.1.2 dostupné na vyžádání při interních auditech nebo auditech třetích stran,

9.4.1.3 každoročně přezkoumávány, aby byla zajištěna jejich konzistence s testovacími postupy.

10. Související politiky a vazby

10.1 Tato politika musí být uplatňována ve vazbě na následující politiky SME, aby byla při testování zachována bezpečnost a soulad:

10.1.1 P2S – Politika rolí a odpovědností v oblasti správy a řízení: Vymezuje, kdo odpovídá za dohled nad vývojem, testováním a odpovědnostmi souvisejícími s oddělením systémů.

10.1.2 P4S – Politika řízení přístupu: Upravuje přidělování, správu a odebírání přihlašovacích údajů pro přístup k testovacím systémům.

10.1.3 P8S – Politika povědomí o bezpečnosti informací a školení: Zajišťuje, aby pracovníci rozuměli rizikům testovacích dat, bezpečným postupům nakládání s nimi a správnému oddělení prostředí.

10.1.4 P13S – Politika klasifikace dat a označování: Podporuje jednoznačnou klasifikaci testovacích dat a usměrňuje strategie anonymizace nebo maskování.

10.1.5 P17S – Politika ochrany dat a soukromí: Zajišťuje soulad s povinnostmi podle GDPR, včetně ochranných opatření pro zpracování a ukládání osobních údajů, a to i v testovacích prostředích.

10.1.6 P24S – Politika bezpečného vývoje: Stanoví celková bezpečnostní očekávání pro vývojové týmy, včetně bezpečného používání dat během testovacích fází.

10.1.7 P30S – Politika reakce na incidenty: Stanoví postup reakce na jakékoli porušení nebo problém zjištěný v testovacím prostředí nebo způsobený nesprávným nakládáním s testovacími daty.

10.2 Tyto politiky tvoří jednotný bezpečnostní rámec na podporu integrity testování, minimalizace dat a plného souladu s ISO/IEC 27001 v rámci vývoje a činností QA.

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 6.1 – Vyžaduje hodnocení rizik a opatření k ošetření rizik, včetně rizik souvisejících s testováním.

11.1.2 Kapitola 8.1 – Vyžaduje plánování a řízení provozních procesů, včetně zřízení prostředí testovacích systémů.

11.2 ISO/IEC 27002

11.2.1 Opatření 8.28 – Vyžaduje, aby organizace chránily testovací data a zajistily, že neobsahují citlivá data ani produkční provozní data.

11.2.2 Opatření 8.29 – Ukládá jednoznačné oddělení vývojových, testovacích a produkčních prostředí.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-11 – Pokrývá očekávání týkající se opatření pro vývoj a testování.

11.3.2 SA-12 – Řeší rizika testování v dodavatelském řetězci a bezpečnostní hodnocení.

11.3.3 SC-32 – Vyžaduje oddělení prostředí a ochranu důvěrnosti a integrity testovacích dat.

11.4 Obecné nařízení EU o ochraně osobních údajů (GDPR)

11.4.1 Článek 5 odst. 1 písm. c) – Vyžaduje minimalizaci údajů, včetně používání pouze nezbytných dat pro testování.

11.4.2 Článek 25 – Vyžaduje ochranu osobních údajů již od návrhu, což zahrnuje i opatření pro testovací prostředí.

11.4.3 Článek 32 – Ukládá bezpečné zpracování osobních údajů ve všech systémech, včetně neprodukčních prostředí.

11.5 Směrnice EU NIS2 (2022/2555)

11.5.1 Článek 21 odst. 2 písm. e), h) – Vyžaduje bezpečný vývoj a testování systémů, zejména tam, kde jsou digitální služby vystaveny kybernetickému riziku.

11.6 Nařízení EU DORA (2022/2554)

11.6.1 Článek 9 – Zdůrazňuje význam digitální provozní odolnosti, včetně bezpečného testování ICT systémů prováděného SME ve finančním sektoru.

11.7 COBIT 2019

11.7.1 BAI07 – Řízení akceptace změn a přechodu do provozu: zahrnuje testovací opatření k ověření nových systémů a nakládání s daty.

11.7.2 DSS05 – Řízení bezpečnostních služeb: vyžaduje testovací a vývojové postupy, které zabraňují zneužití nebo zpřístupnění podnikových dat.