					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P29S					Dokumento pavadinimas: **Testavimo duomenų ir testavimo aplinkų politika**							
Versija: 1.0		Įsigaliojimo data: 01.01.2025			Dokumento savininkas:							
X	Politika		Standartas		Procedūra		Forma		Registras		Kita	

Peržiūrų istorija				
Peržiūros numeris	**Peržiūros data**	**Pakeitimai**	**Peržiūrėjo**	**Proceso savininkas**

Patvirtinimai			
Vardas	**Pareigos**	**Data**	**Parašas**

Suderinta su standartais ir reglamentais

Standartas / reglamentas	Punktas / straipsnis	Pastaba
ISO/IEC 27001:2022	6.1, 8 skyriai	
ISO/IEC 27002:2022	Kontrolės priemonės 8.28–8.29	
NIST SP 800-53 Rev. 5	SA-11, SA-12, SC-32	
ES BDAR	5(1)(c), 25, 32 straipsniai	
ES NIS2 direktyva	21(2)(e), 21(2)(h) straipsniai	
ES DORA reglamentas	9 straipsnis	
COBIT 2019	BAI07, DSS05	

1. Tikslas

1.1 Ši politika nustato testavimo duomenų ir testavimo aplinkų valdymo reikalavimus, kad testavimo veiklos metu būtų išvengta atsitiktinio duomenų atskleidimo, informacijos saugumo incidentų ir veiklos sutrikimų.

1.2 Ji užtikrina, kad programinės įrangos ar sistemų testavimo metu tikri klientų duomenys nebūtų naudojami netinkamai, o testavimo aplinkos būtų logiškai ir techniškai atskirtos nuo produkcinės aplinkos sistemų.

1.3 Ši politika parengta siekiant padėti MVĮ laikytis ISO/IEC 27001 sertifikavimo reikalavimų ir taikomų duomenų apsaugos teisės aktų, kartu užtikrinant, kad ji būtų praktiška ir įgyvendinama organizacijoms, neturinčioms specializuotos IT komandos.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 Visoms testavimo aplinkoms (pvz., parengimo aplinkai serveriuose, smėliadėžės aplinkai, kūrimo testavimo stendams)

2.1.2 Visiems testavimo duomenims, neatsižvelgiant į tai, ar jie sukurti rankiniu būdu, sugeneruoti, ar gauti iš veikiančių duomenų

2.1.3 Visiems asmenims, dalyvaujantiems testavimo veiklose, įskaitant darbuotojus, rangovus, laisvai samdomus specialistus ir IT paslaugų teikėjus

2.1.4 Bet kokiam testavimui, galinčiam paveikti klientams skirtas platformas, vidines verslo sistemas ar trečiųjų šalių paslaugas

2.2 Ji apima technines aplinkas ir procesus, naudojamus šiai veiklai užtikrinti:

2.2.1 Svetainių, taikomųjų programų ir įrankių kūrimui

2.2.2 Sistemų atnaujinimams, konfigūracijos testavimui ir integraciniam testavimui

2.2.3 Automatizuotiems ir rankiniams funkciniams arba saugumo testams

3. Tikslai

3.1 Užkirsti kelią tikrų, identifikuojamų klientų duomenų naudojimui testavime, išskyrus atvejus, kai jie yra anonimizuoti ir aiškiai patvirtinti.

3.2 Užtikrinti griežtą testavimo ir produkcinių sistemų atskyrimą, kad būtų išvengta netyčinio duomenų atskleidimo ar veiklos sutrikimų.

3.3 Apsaugoti testavimo sistemas ir duomenis nuo neteisėtos prieigos, atsitiktinio atskleidimo ar pakartotinio naudojimo skirtingose aplinkose netaikant tinkamų kontrolės priemonių.

3.4 Laikytis taikomų duomenų apsaugos reikalavimų (pvz., ES BDAR, NIS2 direktyvos), užtikrinant, kad visi testavimo duomenys būtų tvarkomi teisėtai, sąžiningai ir saugiai.

3.5 Padėti organizacijai pasirengti išoriniams auditams ir ISO/IEC 27001 sertifikavimui, dokumentuojant testavimo praktikas ir taikant nuoseklias apsaugos priemones.

4. Vaidmenys ir atsakomybės

4.1 Generalinis direktorius (GD)

4.1.1 Atsako už bendrą testavimo duomenų apsaugą ir testavimo sistemų saugumą.

4.1.2 Tvirtina bet kokį tikrų duomenų naudojimą testavime, įsitikinęs, kad taikomos tinkamos apsaugos priemonės (pvz., anonimizavimas ar duomenų maskavimas).

4.1.3 Tikrina, ar testavimo veiklos yra tinkamai dokumentuotos ir atitinka šią politiką.

4.2 Projekto savininkas

4.2.1 Koordinuoja testavimo procesų projektavimą ir vykdymą.

4.2.2 Užtikrina, kad visi komandos nariai suprastų ir laikytųsi šios politikos.

4.2.3 Patvirtina, kad prieš pradedant testavimą testavimo sistemos yra saugiai sukonfigūruotos.

4.2.4 Apie visus incidentus, susijusius su testavimo aplinkomis ar duomenų nutekėjimu, praneša GD.

[... 4.3–8 skyriai nėra įtraukti į šią peržiūrą. Įsigykite visą dokumentą, kad pasiektumėte visą turinį. ...]

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Planinės peržiūros

9.1.1 Ši politika turi būti peržiūrima ne rečiau kaip kartą per metus Generalinio direktoriaus (GD). Peržiūra turi užtikrinti, kad politika išliktų aktuali atsižvelgiant į:

9.1.1.1 Programinės įrangos kūrimo įrankių, platformų ar aplinkų pokyčius

9.1.1.2 Atnaujintus teisinius įpareigojimus, įskaitant duomenų apsaugos ar skaitmeninio operacinio atsparumo reikalavimus

9.1.1.3 MVĮ pasirengimą sertifikavimui ir auditui pagal ISO/IEC 27001

9.2 Tarpinių peržiūrų inicijavimo įvykiai

9.2.1 Papildomos peržiūros turi būti atliekamos po:

9.2.1.1 Bet kokio incidento, susijusio su duomenų atskleidimu ar kompromitavimu testavimo aplinkose

9.2.1.2 Tikrų duomenų naudojimo testavime, net jei jie buvo anonimizuoti

9.2.1.3 Naujų testavimo metodų, sistemų ar tiekėjų įdiegimo

9.2.1.4 Reguliacinių pokyčių, turinčių įtakos duomenų tvarkymui testavimo metu

9.3 Pakeitimų valdymas ir komunikacija

9.3.1 GD atsako už:

9.3.1.1 Šios politikos atnaujinimą ir visų pakeitimų dokumentavimą versijų istorijoje

9.3.1.2 Darbuotojų, kūrėjų ir susijusių paslaugų teikėjų informavimą apie atnaujinimus

9.3.1.3 Patvirtinimą, kad visi su testavimu susiję asmenys supranta ir taiko naujausias taisykles

9.3.1.4 Naujausios politikos versijos prieinamumo užtikrinimą peržiūros ir audito tikslais

9.4 Auditas ir dokumentacija

9.4.1 Visų politikos peržiūrų, tikrų duomenų naudojimo patvirtinimų ir visų išimčių pagrindimų įrašai turi būti:

9.4.1.1 Saugiai saugomi audito tikslais

9.4.1.2 Pateikiami pagal pareikalavimą vidaus ar trečiųjų šalių auditų metu

9.4.1.3 Kasmet peržiūrimi siekiant užtikrinti atitiktį testavimo praktikai

10. Susijusios politikos ir sąsajos

10.1 Ši politika turi būti taikoma kartu su toliau nurodytomis MVĮ politikomis, siekiant užtikrinti saugumą ir atitiktį testavimo metu:

10.1.1 P2S – Valdysenos vaidmenų ir atsakomybių politika: nustato, kas atsakingas už kūrimo, testavimo ir sistemų atskyrimo atsakomybių priežiūrą.

10.1.2 P4S – Prieigos kontrolės politika: reglamentuoja testavimo sistemų prisijungimo duomenų suteikimą, valdymą ir panaikinimą.

10.1.3 P8S – Informacijos saugumo suvokimo ir mokymo politika: užtikrina, kad darbuotojai suprastų testavimo duomenų rizikas, saugaus tvarkymo praktikas ir tinkamą aplinkų atskyrimą.

10.1.4 P13S – Duomenų klasifikavimo ir ženklinimo politika: padeda aiškiai klasifikuoti testavimo duomenis ir nustatyti anonimizavimo ar duomenų maskavimo strategijas.

10.1.5 P17S – Duomenų apsaugos ir privatumo politika: užtikrina suderinamumą su ES BDAR reikalavimais, įskaitant apsaugos priemones, taikomas asmens duomenų tvarkymui ir saugojimui, taip pat testavimo aplinkose.

10.1.6 P24S – Saugaus kūrimo politika: nustato bendruosius saugumo reikalavimus kūrimo komandoms, įskaitant saugų duomenų naudojimą testavimo etapuose.

10.1.7 P30S – Reagavimo į incidentus politika: apibrėžia, kaip reaguoti į bet kokį pažeidimą ar problemą, nustatytą testavimo aplinkoje arba kilusią dėl netinkamo testavimo duomenų tvarkymo.

10.2 Šios politikos sudaro vientisą saugumo sistemą, skirtą užtikrinti testavimo vientisumą, duomenų minimizavimą ir visišką atitiktį ISO/IEC 27001 visose kūrimo ir kokybės užtikrinimo veiklose.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 6.1 punktas – reikalauja atlikti rizikos vertinimą ir taikyti rizikos tvarkymo veiksmus, įskaitant su testavimu susijusias rizikas.

11.1.2 8.1 punktas – reikalauja planuoti ir kontroliuoti operacinius procesus, įskaitant testavimo sistemų ir parengimo aplinkų valdymą.

11.2 ISO/IEC 27002

11.2.1 Kontrolės priemonė 8.28 – reikalauja, kad organizacijos apsaugotų testavimo duomenis ir užtikrintų, kad juose nebūtų jautrių ar veikiančių produkcinių duomenų.

11.2.2 Kontrolės priemonė 8.29 – nustato aiškų kūrimo, testavimo ir produkcinės aplinkos atskyrimą.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-11 – apima kūrimo ir testavimo kontrolės priemonių reikalavimus.

11.3.2 SA-12 – apima tiekimo grandinės testavimo rizikas ir saugumo vertinimus.

11.3.3 SC-32 – reikalauja aplinkų atskyrimo bei testavimo duomenų konfidencialumo ir vientisumo apsaugos.

11.4 Europos Sąjungos Bendrasis duomenų apsaugos reglamentas (BDAR)

11.4.1 5(1)(c) straipsnis – nustato duomenų minimizavimo reikalavimą, įskaitant tik būtinų duomenų naudojimą testavimui.

11.4.2 25 straipsnis – reikalauja užtikrinti duomenų apsaugą pagal projektavimą, kuri apima ir testavimo aplinkų kontrolės priemones.

11.4.3 32 straipsnis – nustato saugaus asmens duomenų tvarkymo reikalavimą visose sistemose, įskaitant neprodukcines aplinkas.

11.5 ES NIS2 direktyva (2022/2555)

11.5.1 21(2)(e), 21(2)(h) straipsniai – reikalauja saugaus kūrimo ir sistemų testavimo, ypač kai skaitmeninėms paslaugoms kyla kibernetinė rizika.

11.6 ES DORA reglamentas (2022/2554)

11.6.1 9 straipsnis – pabrėžia skaitmeninio operacinio atsparumo svarbą, įskaitant saugų IRT sistemų testavimą MVĮ finansų sektoriuje.

11.7 COBIT 2019

11.7.1 BAI07 – valdyti pakeitimų priėmimą ir perdavimą eksploatacijai: apima testavimo kontrolės priemones, skirtas patvirtinti naujas sistemas ir duomenų tvarkymą.

11.7.2 DSS05 – valdyti saugumo paslaugas: nustato testavimo ir kūrimo praktikas, kurios užkerta kelią veiklos duomenų netinkamam naudojimui ar atskleidimui.