					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P29					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	Skyrius / straipsnis	Komentaras
ISO/IEC 27001:2022	8 skyrius	Aktualu saugiam testavimo duomenų ir aplinkų planavimui bei kontrolei
ISO/IEC 27002:2022	Kontrolės priemonės 8.28–8.29	Apima saugius testavimo duomenis ir testavimo aplinkų apsaugą
NIST SP 800-53 Rev. 5	SA-11, SC-28, SC-32	Apima kūrėjų vykdomą testavimą ir vertinimą, saugomų duomenų apsaugą bei vientisumą
ES BDAR	5, 25, 32 straipsniai	Apima duomenų kiekio mažinimą, privatumo užtikrinimą pagal projektavimą ir tvarkymo saugumą testavimo kontekste
ES NIS2 direktyva	21 straipsnio 2 dalies e ir h punktai	Susiję su saugaus kūrimo ir testavimo praktika
ES DORA reglamentas	9 straipsnis	Susiję su IRT sistemomis ir protokolais bei testavimo duomenų saugumu
COBIT 2019	DSS05, BAI07	Apima saugumo paslaugų valdymą ir pakeitimų priėmimą bei perėjimą

1. Tikslas

1.1. Ši politika nustato privalomuosius reikalavimus testavimo aplinkų ir testavimo duomenų valdymui, siekiant užtikrinti saugumą, konfidencialumą ir veiklos vientisumą viso programinės įrangos kūrimo ir testavimo gyvavimo ciklo metu.

1.2. Ja siekiama užkirsti kelią neteisėtai prieigai, duomenų iškėlimui ir produkcinių sistemų užteršimui dėl netinkamai valdomų testavimo aplinkų arba realių duomenų naudojimo testavimui.

1.3. Ši politika nustato saugų testavimui naudojamų duomenų tvarkymą, testavimo infrastruktūros saugumo stiprinimą ir vaidmenimis grindžiamą prieigos kontrolę, kartu užtikrinant atitiktį taikomiems reguliavimo ir sutartiniams įpareigojimams.

2. Taikymo sritis

2.1. Ši politika taikoma visoms testavimo aplinkoms, duomenims, priemonėms ir procesams, naudojamiems organizacijoje programinės įrangos, sistemų, taikomųjų programų ir infrastruktūros testavimui.

2.2. Politika apima:

2.2.1. Testavimo aplinkas, įdiegtas vietinėje infrastruktūroje, debesijos aplinkose arba trečiųjų šalių platformose

2.2.2. Testavimo duomenis, naudojamus funkciniam, našumo, regresiniam ir saugumo testavimui

2.2.3. Rankinį, scenarijais grindžiamą arba automatizuotą testavimą (pvz., CI/CD konvejerius)

2.2.4. Visą personalą, dalyvaujantį testavime, įskaitant vidines komandas, tiekėjus ir rangovus

2.3. Ši politika taikoma nepriklausomai nuo sistemos kritiškumo, taikomosios programos tipo ar to, ar kūrimas vykdomas viduje, ar perduotas išorės paslaugų teikėjams.

3. Tikslai

3.1. Užkirsti kelią aktyvių, jautrių ar reglamentuojamų duomenų (pvz., asmens tapatybę identifikuojančios informacijos (AII), kortelių turėtojų duomenų) naudojimui testavimo aplinkose, išskyrus atvejus, kai jie yra anonimizuoti arba tam yra gautas konkretus patvirtinimas.

3.2. Užtikrinti visišką tinklo ir prieigos atskyrimą tarp testavimo ir produkcinių aplinkų, kad būtų išvengta neteisėtos prieigos prie duomenų ar sistemų užteršimo.

3.3. Nustatyti privalomą šifravimo, duomenų maskavimo arba sintetinių duomenų generavimo taikymą, kai testavimui reikalingi reprezentatyvūs duomenys.

3.4. Sumažinti atitikties pažeidimų, klientų duomenų atskleidimo ar veiklos sutrikimų tikimybę, kylančią dėl nesaugių testavimo duomenų ar aplinkų.

3.5. Suderinti testavimo duomenų tvarkymą su pramonės gerąja praktika, standartais (ISO, NIST, COBIT) ir reglamentais, tokiais kaip ES BDAR, NIS2 direktyva ir DORA reglamentas.

4. Vaidmenys ir atsakomybės

4.1. Informacijos saugumo vadovas (CISO)

4.1.1. Yra šios politikos savininkas ir užtikrina techninių bei administracinių apsaugos priemonių taikymą testavimo duomenims ir aplinkoms.

4.1.2. Tvirtina realių ar jautrių duomenų naudojimą testavime, kai pateikiamas tinkamas pagrindimas ir taikomos kompensuojamosios kontrolės priemonės.

4.2. Kokybės užtikrinimo (QA) / testavimo vadovai

4.2.1. Koordinuoja testavimo planavimą ir užtikrina, kad visa testavimo veikla atitiktų šios politikos reikalavimus.

4.2.2. Patvirtina tinkamą atskyrimą, prieigą ir duomenų parengimą kiekvienam testavimo etapui.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1. Ši politika turi būti peržiūrima kasmet ir prireikus atnaujinama, kad atspindėtų:

9.1.1. Reglamentavimo reikalavimų pokyčius (pvz., ES BDAR, DORA reglamentą, NIS2 direktyvą)

9.1.2. Naujų testavimo priemonių, platformų arba automatizavimo konvejerių diegimą

9.1.3. Vidaus audito išvadas arba poincidentines rekomendacijas

9.1.4. Kūrimo arba QA procesų plėtrą, keičiančią testavimo duomenų tvarkymą arba aplinkų naudojimą

9.2. CISO yra atsakingas už peržiūros inicijavimą bendradarbiaujant su:

9.2.1. QA / testavimo vadovais

9.2.2. „DevOps“ ir infrastruktūros vadovais

9.2.3. Taikomųjų programų kūrimo komandomis

9.2.4. Duomenų apsaugos pareigūnu (DAP) ir teisininku

9.3. Visi pakeitimai turi būti:

9.3.1. Valdomi pagal versijų kontrolę ir saugomi centrinėje dokumentų saugykloje

9.3.2. Pranešami susijusiam personalui oficialiais kanalais (pvz., ISVS pranešimais, komandų instruktažais)

9.3.3. Susieti su susijusių techninių standartų, kontrolės priemonių ir veiklos procedūrų atnaujinimais

9.4. Tarpinės peržiūros pagal suveikimo įvykius turi būti atliekamos nedelsiant po bet kurio iš šių atvejų:

9.4.1. Duomenų iškėlimo arba duomenų saugumo pažeidimo, susijusio su testavimo aplinkomis

9.4.2. Audito neatitikties, susijusios su testavimo duomenų tvarkymu

9.4.3. Reikšmingų teisinių įpareigojimų arba IT architektūros pokyčių

10. Susijusios politikos ir sąsajos

10.1. Ši politika yra glaudžiai susijusi su toliau nurodytomis politikomis, siekiant užtikrinti saugų ir reikalavimus atitinkantį testavimo duomenų bei aplinkų tvarkymą:

10.1.1. P1 – Informacijos saugumo politika: nustato bendruosius saugumo principus, reglamentuojančius testavimo duomenų apsaugą ir aplinkų valdymą.

10.1.2. P5 – Pakeitimų valdymo politika: taikoma testavimo aplinkų kūrimui, atnaujinimui, eksploatacijos nutraukimui ir diegimo konvejeriams.

10.1.3. P13 – Duomenų klasifikavimo ir ženklinimo politika: nustato testavimo duomenų parinkimo gaires ir pagal jautrumą taikomas kontrolės priemones.

10.1.4. P14 – Duomenų saugojimo ir sunaikinimo politika: nustato testavimo duomenų rinkinių saugojimo terminus ir saugaus sunaikinimo reikalavimus.

10.1.5. P15 – Atsarginių kopijų ir atkūrimo politika: nustato privalomąsias atsarginių kopijų kūrimo praktikas ir atkūrimo validavimą testavimo aplinkoms.

10.1.6. P18 – Kriptografinių kontrolės priemonių politika: nustato privalomuosius šifravimo standartus saugomiems ir perduodamiems duomenims testavimo platformose.

10.1.7. P22 – Žurnalų tvarkymo ir stebėsenos politika: reglamentuoja matomumą ir anomalijų aptikimą testavimo aplinkų veikloje.

10.1.8. P30 – Reagavimo į incidentus politika: nustato eskalavimo ir taisomųjų veiksmų tvarką pažeidimų ar incidentų, susijusių su testavimo sistemomis, atveju.

10.1.9. P33 – Audito ir atitikties stebėsenos politika: sudaro sąlygas politikos laikymosi validavimui ir nuolatiniam užtikrinimui.

11. Pamatiniai standartai ir sistemos

11.1. Ši politika yra suderinta su pasauliniais kibernetinio saugumo standartais ir reglamentavimo sistemomis, kurios nustato saugaus testavimo duomenų tvarkymo ir neprodukcinės aplinkos apsaugos reikalavimus.

11.2. ISO/IEC 27001:

11.2.1. 8.1 skyrius – nustato saugaus testavimo duomenų ir aplinkų planavimo bei kontrolės reikalavimus.

11.3. ISO/IEC 27002:2022 – kontrolės priemonės 8.28–8.29:

11.3.1. A priedo kontrolės priemonė 8.28 – saugūs testavimo duomenys: reikalauja kūrimo ir testavimo etapuose naudojamų testavimo duomenų apsaugos taikant anonimizavimą, duomenų maskavimą arba sintetinių duomenų generavimą.

11.3.2. A priedo kontrolės priemonė 8.29 – testavimo aplinkų apsauga: reikalauja atskyrimo nuo produkcinių aplinkų, prieigos kontrolės ir aplinkų saugumo stiprinimo testavimo sistemoms.

11.3.3. Šios kontrolės priemonės nustato saugaus testavimo metu naudojamų duomenų valdymo ir neprodukcinės sistemos apsaugos nuo netinkamo naudojimo, kompromitavimo ar užteršimo reikalavimus.

11.4. NIST SP 800-53 Rev. 5:

11.4.1. SA-11 – kūrėjų testavimas ir vertinimas: nustato saugių, pakartojamų testavimo procedūrų su tinkamomis duomenų kontrolės priemonėmis lūkesčius.

11.4.2. SC-28 – saugomų duomenų apsauga: atitinka testavimo duomenų, saugomų neprodukcinėse sistemose, šifravimo reikalavimus.

11.4.3. SC-32 – informacijos vientisumas: palaiko duomenų validavimą, apsaugą nuo sugadinimo ir įvesties / išvesties kontrolės priemones testavimo metu.

11.5. ES BDAR (2016/679):

11.5.1. 5 straipsnis – duomenų kiekio mažinimas: draudžia nebūtiną asmens duomenų naudojimą testavime.

11.5.2. 25 straipsnis – privatumas pagal projektavimą: reikalauja taikyti duomenų apsaugos metodus nuo pat kūrimo ir testavimo ciklo pradžios.

11.5.3. 32 straipsnis – tvarkymo saugumas: nustato apsaugos priemonių reikalavimą testavimo aplinkoms, kuriose tvarkomi asmens ar jautrūs duomenys.

11.6. ES NIS2 direktyva (2022/2555):

11.6.1. 21 straipsnio 2 dalies e ir h punktai: reikalauja saugių programinės įrangos kūrimo ir testavimo procesų, akcentuojant apsaugą nuo neteisėtos prieigos ir duomenų iškėlimo.

11.7. ES DORA reglamentas (2022/2554):

11.7.1. 9 straipsnis – IRT sistemos ir protokolai: reikalauja, kad testavimo procesai palaikytų atsparumą ir saugotų operacinius duomenis nuo kompromitavimo ar neautorizuoto atskleidimo.

11.8. COBIT 2019:

11.8.1. DSS05 – saugumo paslaugų valdymas: palaiko saugumo politikų taikymą visose aplinkose, įskaitant neprodukcinę aplinką.

11.8.2. BAI07 – pakeitimų priėmimo ir perėjimo valdymas: apima formalų perėjimo iš testavimo į produkcinę aplinką procesą, įskaitant duomenų ir aplinkų kontrolės priemones.