					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P29S					Dokumenta nosaukums: **Testa datu un testa vides politika**							
Versija: 1.0		Spēkā stāšanās datums: 01.01.2025			Dokumenta īpašnieks:							
X	Politika		Standarts		Procedūra		Veidlapa		Reģistrs		Cits	

Pārskatījumu vēsture				
Pārskatījuma numurs	**Pārskatījuma datums**	**Izmaiņas**	**Pārskatīja**	**Procesa īpašnieks**

Apstiprinājumi			
Vārds	**Amats**	**Datums**	**Paraksts**

Saskaņošana ar piemērojamajiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	Punkti 6.1, 8	
ISO/IEC 27002:2022	Kontroles pasākumi 8.28–8.29	
NIST SP 800-53 Rev. 5	SA-11, SA-12, SC-32	
ES VDAR	Panti 5(1)(c), 25, 32	
ES NIS2	Pants 21(2)(e), (h)	
ES DORA	Pants 9	
COBIT 2019	BAI07, DSS05	

1. Mērķis

1.1 Šī politika nosaka prasības testa datu un testa vidu pārvaldībai, lai testēšanas darbību laikā novērstu nejaušu informācijas izpaušanu, datu aizsardzības pārkāpumus un darbības traucējumus.

1.2 Tā nodrošina, ka programmatūras vai sistēmu testēšanā reāli klientu dati netiek izmantoti neatbilstoši un ka testa vides ir loģiski un tehniski nodalītas no ražošanas vidēm.

1.3 Politika ir izstrādāta, lai palīdzētu MVU izpildīt ISO/IEC 27001 sertifikācijas prasības un piemērojamo datu aizsardzības tiesību aktu prasības, vienlaikus saglabājot tās praktisku ieviešanu un piemērošanu organizācijās bez īpaši izveidotas IT komandas.

2. Piemērošanas joma

2.1 Šī politika attiecas uz:

2.1.1 visām testa vidēm (piemēram, sagatavošanas serveriem, smilškastes sistēmām, izstrādes un testēšanas vidēm);

2.1.2 visiem testa datiem neatkarīgi no tā, vai tie ir izveidoti manuāli, ģenerēti vai atvasināti no ražošanas vidē izmantotajiem datiem;

2.1.3 visu personālu, kas iesaistīts testēšanas darbībās, tostarp darbiniekiem, līgumslēdzējiem, ārštata speciālistiem un IT pakalpojumu sniedzējiem;

2.1.4 jebkuru testēšanu, kas var ietekmēt klientiem pieejamās platformas, iekšējās biznesa sistēmas vai trešo pušu pakalpojumus.

2.2 Tā aptver gan tehniskās vides, gan procesus, ko izmanto, lai nodrošinātu:

2.2.1 tīmekļvietņu, lietotņu un rīku izstrādi;

2.2.2 sistēmu atjauninājumu, konfigurāciju un integrāciju testēšanu;

2.2.3 automatizētus un manuālus funkcionālos vai drošības testus.

3. Mērķi

3.1 Novērst reālu, identificējamu klientu datu izmantošanu testēšanā, ja vien tie nav anonimizēti un nav saņemts nepārprotams apstiprinājums.

3.2 Uzturēt stingru nodalījumu starp testa un ražošanas vidēm, lai nepieļautu neparedzētu datu izpaušanu vai ietekmi uz darbību.

3.3 Aizsargāt testa sistēmas un datus pret neatļautu piekļuvi, nejaušu izpaušanu vai atkārtotu izmantošanu dažādās vidēs bez atbilstošiem kontroles pasākumiem.

3.4 Nodrošināt atbilstību piemērojamajām datu aizsardzības prasībām (piemēram, VDAR, NIS2), nodrošinot, ka visi testa dati tiek apstrādāti likumīgi, godprātīgi un droši.

3.5 Atbalstīt organizācijas gatavību ārējiem auditiem un ISO/IEC 27001 sertifikācijai, dokumentējot testēšanas praksi un konsekventi piemērojot drošības pasākumus.

4. Lomas un pienākumi

4.1 Ģenerāldirektors (GM)

4.1.1 Ir vispārīgi atbildīgs par testa datu aizsardzību un testa sistēmu drošību.

4.1.2 Apstiprina jebkādu reālu datu izmantošanu testēšanā pēc pārliecināšanās par atbilstošu drošības pasākumu piemērošanu (piemēram, anonimizāciju vai datu maskēšanu).

4.1.3 Pārbauda, vai testēšanas darbības ir pienācīgi dokumentētas un atbilst šai politikai.

4.2 Projekta īpašnieks

4.2.1 Koordinē testēšanas procesu izstrādi un izpildi.

4.2.2 Nodrošina, ka visi komandas locekļi izprot un ievēro šo politiku.

4.2.3 Pirms testēšanas sākuma apstiprina, ka testa sistēmas ir droši konfigurētas.

4.2.4 Ziņo GM par jebkuriem incidentiem, kas saistīti ar testa vidēm vai datu noplūdēm.

[... Sadaļas 4.3–8 nav iekļautas šajā priekšskatījumā. Iegādājieties pilnu dokumentu, lai piekļūtu pilnam saturam. ...]

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Plānotā pārskatīšana

9.1.1 Šī politika ģenerāldirektoram (GM) jāpārskata vismaz reizi gadā. Pārskatīšanas mērķis ir nodrošināt, ka politika saglabā aktualitāti attiecībā uz:

9.1.1.1 izmaiņām programmatūras izstrādes rīkos, platformās vai vidēs;

9.1.1.2 atjauninātām tiesiskajām prasībām, tostarp datu aizsardzības vai digitālās noturības jomā;

9.1.1.3 MVU sertifikācijas prasībām un gatavību auditam saskaņā ar ISO/IEC 27001.

9.2 Starpposma pārskatīšanas ierosinātāji

9.2.1 Papildu pārskatīšana jāveic pēc:

9.2.1.1 jebkura incidenta, kas saistīts ar datu izpaušanu vai kompromitēšanu testa vidēs;

9.2.1.2 reālu datu izmantošanas testēšanā, pat ja tie ir anonimizēti;

9.2.1.3 jaunu testēšanas metožu, sistēmu vai piegādātāju ieviešanas;

9.2.1.4 normatīvo prasību izmaiņām, kas ietekmē datu apstrādi testēšanas laikā.

9.3 Izmaiņu pārvaldība un komunikācija

9.3.1 GM ir atbildīgs par:

9.3.1.1 šīs politikas atjaunināšanu un visu grozījumu dokumentēšanu, uzturot versiju vēsturi;

9.3.1.2 darbinieku, izstrādātāju un attiecīgo pakalpojumu sniedzēju informēšanu par atjauninājumiem;

9.3.1.3 apstiprināšanu, ka viss ar testēšanu saistītais personāls izprot un piemēro jaunākās prasības;

9.3.1.4 aktuālās politikas versijas pieejamības nodrošināšanu pārskatīšanas un audita vajadzībām.

9.4 Audits un dokumentācija

9.4.1 Ierakstiem par visām politikas pārskatīšanām, reālu datu izmantošanas apstiprinājumiem un visu izņēmumu pamatojumiem jābūt:

9.4.1.1 droši glabātiem audita vajadzībām;

9.4.1.2 pieejamiem pēc pieprasījuma iekšējo vai trešo pušu auditu laikā;

9.4.1.3 reizi gadā pārskatītiem, lai nodrošinātu atbilstību testēšanas praksei.

10. Saistītās politikas un sasaiste

10.1 Šī politika jāpiemēro kopā ar šādām MVU politikām, lai testēšanas laikā uzturētu drošību un atbilstību:

10.1.1 P2S – Pārvaldības lomu un atbildības politika: nosaka, kurš ir atbildīgs par izstrādes, testēšanas un sistēmu nodalīšanas pienākumu pārraudzību.

10.1.2 P4S – Piekļuves kontroles politika: reglamentē piekļuves un autentifikācijas datu piešķiršanu, pārvaldību un atsaukšanu testa sistēmām.

10.1.3 P8S – Informācijas drošības informētības un apmācības politika: nodrošina, ka personāls izprot testa datu riskus, drošas apstrādes praksi un pareizu vides nodalīšanu.

10.1.4 P13S – Datu klasifikācijas un marķēšanas politika: atbalsta skaidru testa datu klasifikāciju un nosaka anonimizācijas vai datu maskēšanas pieejas.

10.1.5 P17S – Datu aizsardzības un privātuma politika: nodrošina saskaņotību ar VDAR prasībām, tostarp attiecībā uz personas datu apstrādes un glabāšanas drošības pasākumiem arī testa vidēs.

10.1.6 P24S – Drošas izstrādes politika: nosaka vispārējās drošības prasības izstrādes komandām, tostarp drošu datu izmantošanu testēšanas posmos.

10.1.7 P30S – Incidentu pārvaldības politika: nosaka, kā reaģēt uz jebkuru pārkāpumu vai problēmu, kas konstatēta testa vidē vai radusies neatbilstošas testa datu apstrādes dēļ.

10.2 Šīs politikas kopā veido vienotu drošības ietvaru, lai atbalstītu testēšanas integritāti, datu minimizēšanu un pilnīgu atbilstību ISO/IEC 27001 izstrādes un kvalitātes nodrošināšanas darbībās.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 Punkts 6.1 – nosaka risku izvērtēšanas un riska apstrādes darbības, tostarp ar testēšanu saistītos riskus.

11.1.2 Punkts 8.1 – nosaka darbības procesu plānošanu un kontroli, tostarp testa sistēmu izveides un uzturēšanas vidi.

11.2 ISO/IEC 27002

11.2.1 Kontroles pasākums 8.28 – nosaka prasību organizācijām aizsargāt testa datus un nodrošināt, ka tie nesatur sensitīvus datus vai reālus ražošanas vides datus.

11.2.2 Kontroles pasākums 8.29 – nosaka skaidru izstrādes, testēšanas un ražošanas vides nodalīšanu.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-11 – aptver izstrādes un testēšanas kontroles pasākumu prasības.

11.3.2 SA-12 – attiecas uz piegādes ķēdes testēšanas riskiem un drošības izvērtējumiem.

11.3.3 SC-32 – nosaka vides nodalīšanu un testa datu konfidencialitātes un integritātes aizsardzību.

11.4 Eiropas Savienības Vispārīgā datu aizsardzības regula (VDAR)

11.4.1 Pants 5(1)(c) – nosaka datu minimizēšanu, tostarp tikai nepieciešamo datu izmantošanu testēšanai.

11.4.2 Pants 25 – nosaka datu aizsardzību pēc projektēšanas un pēc noklusējuma, kas ietver arī testa vides kontroles pasākumus.

11.4.3 Pants 32 – nosaka drošu personas datu apstrādi visās sistēmās, tostarp neprodukcijas vidēs.

11.5 ES NIS2 direktīva (2022/2555)

11.5.1 Pants 21(2)(e, h) – nosaka drošu izstrādi un sistēmu testēšanu, jo īpaši gadījumos, kad digitālie pakalpojumi ir pakļauti kiberriskam.

11.6 ES DORA regula (2022/2554)

11.6.1 Pants 9 – uzsver digitālās darbības noturības nozīmi, tostarp drošu IKT sistēmu testēšanu MVU finanšu sektorā.

11.7 COBIT 2019

11.7.1 BAI07 – pārvaldīt izmaiņu pieņemšanu un pāreju: ietver testēšanas kontroles pasākumus jaunu sistēmu un datu apstrādes validēšanai.

11.7.2 DSS05 – pārvaldīt drošības pakalpojumus: nosaka testēšanas un izstrādes praksi, kas novērš biznesa datu neatbilstošu izmantošanu vai izpaušanu.