					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P29					Dokumenta nosaukums: **Testa datu un testa vidi 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**

Saskaņots ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	8. punkts	Attiecas uz drošu testa datu un testa vidi plānošanu un kontroli
ISO/IEC 27002:2022	8.28–8.29 kontroles pasākumi	Aptver drošu testa datu un testa vidi aizsardzību
NIST SP 800-53 Rev.5	SA-11, SC-28, SC-32	Attiecas uz izstrādātāju testēšanu un izvērtēšanu, datu aizsardzību glabāšanā un integritāti
ES GDPR	5., 25., 32. pants	Aptver datu minimizēšanu, datu aizsardzību pēc projektēšanas un apstrādes drošību testēšanas kontekstā
ES NIS2	21. panta 2. punkta e) un h) apakšpunkts	Attiecas uz drošas izstrādes un testēšanas praksi
ES DORA	9. pants	Attiecas uz IKT sistēmām un protokoliem, kā arī testa datu drošību
COBIT 2019	DSS05, BAI07	Attiecas uz drošības pakalpojumu pārvaldību un izmaiņu pieņemšanu/pāreju

1. Mērķis

1.1. Šī politika nosaka obligātās prasības testa vidi un testa datu pārvaldībai, lai visā programmatūras izstrādes un testēšanas dzīves ciklā nodrošinātu drošību, konfidencialitāti un darbības integritāti.

1.2. Tās mērķis ir novērst neautorizētu piekļuvi, datu noplūdes un ražošanas sistēmu kontaminmāciju, ko rada neatbilstoši pārvaldītas testa vides vai reālu datu izmantošana testēšanā.

1.3. Šī politika nosaka drošu testēšanā izmantoto datu apstrādi, drošu testa infrastruktūras konfigurēšanu un lomu balstītu piekļuves kontroli, vienlaikus nodrošinot atbilstību piemērojamajām normatīvajām un līgumiskajām prasībām.

2. Piemērošanas joma

2.1. Šī politika attiecas uz visām testa vidēm, datiem, rīkiem un procesiem, kas organizācijā tiek izmantoti programmatūras, sistēmu, lietotņu un infrastruktūras testēšanai.

2.2. Tā aptver:

2.2.1. Testa vides, kas tiek nodrošinātas lokāli, mākoņvidē vai ar trešo pušu platformu starpniecību

2.2.2. Testa datus, kas tiek izmantoti funkcionālajā, veiktspējas, regresijas un drošības testēšanā

2.2.3. Manuālu, skriptētu vai automatizētu testēšanu (piemēram, CI/CD cauruļvados)

2.2.4. Visu testēšanā iesaistīto personālu, tostarp iekšējās komandas, piegādātājus un līgumslēdzējus

2.3. Politika ir piemērojama neatkarīgi no sistēmas kritiskuma, lietotnes veida vai tā, vai izstrāde tiek veikta iekšēji vai ārpakalpojumā.

3. Mērķi

3.1. Novērst aktīvu, sensitīvu vai regulētu datu (piemēram, personu identificējošas informācijas (PII), karšu turētāju datu) izmantošanu testa vidēs, ja vien tie nav anonimizēti vai nav saņemts īpašs apstiprinājums.

3.2. Nodrošināt pilnīgu tīkla un piekļuves nodalīšanu starp testa un ražošanas vidēm, lai nepieļautu neautorizētu piekļuvi datiem vai sistēmu kontamināciju.

3.3. Noteikt prasību izmantot šifrēšanu, maskēšanu vai sintētisko datu ģenerēšanu, ja testēšanas vajadzībām ir nepieciešami reprezentatīvi dati.

3.4. Samazināt neatbilstības, klientu datu ekspozīcijas vai darbības traucējumu risku, kas rodas nedrošu testa datu vai testa vidi dēļ.

3.5. Nodrošināt testa datu apstrādes atbilstību nozares standartiem (ISO, NIST, COBIT) un regulējumam, piemēram, GDPR, NIS2 un DORA.

4. Lomas un pienākumi

4.1. Galvenais informācijas drošības vadītājs (CISO)

4.1.1. Ir šīs politikas īpašnieks un nodrošina testa datiem un testa vidēm piemērojamo tehnisko un administratīvo drošības pasākumu ieviešanu.

4.1.2. Apstiprina reālu vai sensitīvu datu izmantošanu testēšanā, ja tam ir atbilstošs pamatojums un noteikti kompensējošie kontroles pasākumi.

4.2. QA/testēšanas vadītāji

4.2.1. Koordinē testēšanas plānošanu un nodrošina, ka visas testēšanas darbības atbilst šīs politikas prasībām.

4.2.2. Validē atbilstošu nodalīšanu, piekļuvi un datu sagatavošanu katram testēšanas posmam.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1. Šī politika jāpārskata reizi gadā un pēc nepieciešamības jāatjaunina, lai atspoguļotu:

9.1.1. Izmaiņas normatīvajās prasībās (piemēram, GDPR, DORA, NIS2)

9.1.2. Jaunu testēšanas rīku, platformu vai automatizācijas cauruļvadu ieviešanu

9.1.3. Iekšējā audita konstatējumus vai pēcincidenta ieteikumus

9.1.4. Izstrādes vai QA procesu paplašināšanu, kas maina testa datu apstrādi vai testa vidi izmantošanu

9.2. CISO ir atbildīgs par pārskatīšanas uzsākšanu sadarbībā ar:

9.2.1. QA/testēšanas vadītājiem

9.2.2. DevOps un infrastruktūras vadītājiem

9.2.3. Lietotņu izstrādes komandām

9.2.4. Datu aizsardzības speciālistu un juridisko konsultantu

9.3. Visiem grozījumiem jābūt:

9.3.1. Pārvaldītiem ar versiju kontroli un glabātiem centrālajā dokumentu repozitorijā

9.3.2. Paziņotiem skartajam personālam, izmantojot formālus kanālus (piemēram, IDPS paziņojumus, komandu instruktāžas)

9.3.3. Saistītiem ar atjauninājumiem attiecīgajos tehniskajos standartos, kontroles pasākumos un darbības procedūrās

9.4. Starpposma pārskatīšana, ko ierosina konkrēti notikumi, jāveic nekavējoties pēc:

9.4.1. Datu noplūdes vai pārkāpuma, kas skar testa vides

9.4.2. Audita neatbilstības saistībā ar testa datu apstrādi

9.4.3. Būtiskām izmaiņām tiesiskajos pienākumos vai IT arhitektūrā

10. Saistītās politikas un sasaiste

10.1. Lai nodrošinātu drošu un atbilstošu testa datu un testa vidi apstrādi, šī politika ir cieši saistīta ar šādām politikām:

10.1.1. P1 – Informācijas drošības politika: nosaka vispārīgos drošības principus, kas regulē testa datu aizsardzību un testa vidi pārvaldību.

10.1.2. P5 – Izmaiņu pārvaldības politika: attiecas uz testa vidi izveidi, atjaunināšanu, izņemšanu no ekspluatācijas un izvietošanas cauruļvadiem.

10.1.3. P13 – Datu klasifikācijas un marķēšanas politika: nosaka vadlīnijas testa datu atlasei un uz sensitivitāti balstītu kontroles pasākumu piemērošanai.

10.1.4. P14 – Datu uzglabāšanas un likvidēšanas politika: nosaka glabāšanas termiņus un drošas likvidēšanas prasības testa datu kopām.

10.1.5. P15 – Rezerves kopiju veidošanas un atjaunošanas politika: nosaka rezerves kopiju veidošanas praksi un atjaunošanas validāciju testa vidēm.

10.1.6. P18 – Kriptogrāfisko kontroles pasākumu politika: nosaka obligātos šifrēšanas standartus datiem glabāšanā un pārsūtē testa platformās.

10.1.7. P22 – Žurnālfiksēšanas un uzraudzības politika: regulē redzamību un anomāliju noteikšanu testa vidi darbībās.

10.1.8. P30 – Incidentu reaģēšanas politika: nosaka eskalāciju un seku novēršanas pasākumus pārkāpumiem vai incidentiem, kas skar testa sistēmas.

10.1.9. P33 – Audita un atbilstības uzraudzības politika: nodrošina politikas ievērošanas validāciju un nepārtrauktu apliecinājumu.

11. Atsauces standarti un ietvari

11.1. Šī politika atbilst globālajiem kiberdrošības standartiem un regulatīvajiem ietvariem, kas nosaka drošu testa datu apstrādi un neprodukcijas vidi aizsardzību.

11.2. ISO/IEC 27001:

11.2.1. 8.1. punkts – nosaka drošu testa datu un testa vidi plānošanu un kontroli.

11.3. ISO/IEC 27002:2022 – 8.28–8.29 kontroles pasākumi:

11.3.1. A pielikuma 8.28. kontrole – droši testa dati: nosaka prasību aizsargāt izstrādes un testēšanas posmos izmantotos testa datus, izmantojot anonimizāciju, maskēšanu vai sintētisku ģenerēšanu.

11.3.2. A pielikuma 8.29. kontrole – testa vidi aizsardzība: nosaka prasību testa sistēmām nodrošināt nodalīšanu no ražošanas vides, piekļuves kontroli un drošu konfigurēšanu.

11.3.3. Šie kontroles pasākumi nosaka prasības drošai testēšanā izmantoto datu pārvaldībai un neprodukcijas sistēmu aizsardzībai pret nepareizu lietošanu, kompromitēšanu vai kontaminmāciju.

11.4. NIST SP 800-53 Rev.5:

11.4.1. SA-11 – izstrādātāju testēšana un izvērtēšana: nosaka prasības drošām, atkārtojamām testēšanas procedūrām ar atbilstošiem datu kontroles pasākumiem.

11.4.2. SC-28 – informācijas aizsardzība glabāšanā: atbilst neprodukcijas sistēmās glabāto testa datu šifrēšanai.

11.4.3. SC-32 – informācijas integritāte: atbalsta datu validāciju, bojājumu novēršanu un ievades/izvades kontroles pasākumus testēšanas laikā.

11.5. ES GDPR (2016/679):

11.5.1. 5. pants – datu minimizēšana: aizliedz nevajadzīgu personas datu izmantošanu testēšanā.

11.5.2. 25. pants – datu aizsardzība pēc projektēšanas: nosaka prasību piemērot datu aizsardzības paņēmienus jau no izstrādes un testēšanas cikla sākuma.

11.5.3. 32. pants – apstrādes drošība: nosaka drošības pasākumus testa vidēm, kurās tiek apstrādāti personas dati vai sensitīvi dati.

11.6. ES NIS2 direktīva (2022/2555):

11.6.1. 21. panta 2. punkta e) un h) apakšpunkts: nosaka drošus programmatūras izstrādes un testēšanas procesus, uzsverot aizsardzību pret neautorizētu piekļuvi un datu noplūdēm.

11.7. ES DORA (2022/2554):

11.7.1. 9. pants – IKT sistēmas un protokoli: nosaka prasību, lai testēšanas procesi veicinātu noturību un aizsargātu darbības datus pret kompromitēšanu vai neautorizētu izpaušanu.

11.8. COBIT 2019:

11.8.1. DSS05 – drošības pakalpojumu pārvaldība: atbalsta drošības politiku piemērošanu visās vidēs, tostarp neprodukcijas vidēs.

11.8.2. BAI07 – izmaiņu pieņemšanas un pārejas pārvaldība: aptver formālu pārejas procesu no testēšanas uz ražošanas vidi, tostarp datu un vidi kontroles pasākumus.