					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P29S					Asiakirjan nimi: **Testidataa ja testiympäristöjä koskeva politiikka**							
Versio: 1.0		Voimaantulopäivä: 01.01.2025			Asiakirjan omistaja:							
X	Politiikka		Standardi		Menettely		Lomake		Rekisteri		Muu	

Muutoshistoria				
Muutosnumero	**Muutospäivä**	**Muutokset**	**Tarkistanut**	**Prosessin omistaja**

Hyväksynnät			
Nimi	**Tehtävänimike**	**Päivämäärä**	**Allekirjoitus**

Yhdenmukaisuus standardien ja sääntelyvaatimusten kanssa

Standardi/sääntely	Kohta/artikla	Kommentti
ISO/IEC 27001:2022	Kohdat 6.1, 8	
ISO/IEC 27002:2022	Kontrollit 8.28–8.29	
NIST SP 800-53 Rev.5	SA-11, SA-12, SC-32	
EU:n GDPR	Artiklat 5(1)(c), 25, 32	
EU:n NIS2-direktiivi	Artikla 21(2)(e), (h)	
EU:n DORA-asetus	Artikla 9	
COBIT 2019	BAI07, DSS05	

1. Tarkoitus

1.1 Tässä politiikassa määritellään, miten testidataa ja testiympäristöjä on hallittava tahattoman altistumisen, tietoturvaloukkausten ja toiminnallisten häiriöiden estämiseksi testaustoiminnan aikana.

1.2 Tällä politiikalla varmistetaan, ettei aitoa asiakasdataa koskaan käytetä ohjelmisto- tai järjestelmätestauksessa epäasianmukaisesti ja että testiympäristöt erotetaan loogisesti ja teknisesti tuotantoympäristöistä.

1.3 Politiikan tarkoituksena on tukea pk-yrityksiä ISO/IEC 27001 -sertifioinnin vaatimusten ja sovellettavan tietosuojalainsäädännön noudattamisessa siten, että vaatimukset pysyvät käytännöllisinä ja toimeenpantavina myös organisaatioissa, joilla ei ole erillistä IT-tiimiä.

2. Soveltamisala

2.1 Tätä politiikkaa sovelletaan seuraaviin:

2.1.1 kaikkiin testiympäristöihin (esim. staging-palvelimet, sandbox-ympäristöt, kehityksen testiympäristöt)

2.1.2 kaikkeen testidataan riippumatta siitä, onko se luotu manuaalisesti, generoitu vai johdettu tuotantodatasta

2.1.3 kaikkiin testaustoimintaan osallistuviin henkilöihin, mukaan lukien työntekijät, sopimuskumppanit, freelancerit ja IT-palveluntarjoajat

2.1.4 kaikkeen testaukseen, joka voi vaikuttaa asiakasrajapinnan alustoihin, sisäisiin liiketoimintajärjestelmiin tai kolmansien osapuolten palveluihin

2.2 Politiikka kattaa sekä tekniset ympäristöt että prosessit, joilla tuetaan seuraavia:

2.2.1 verkkosivustojen, sovellusten ja työkalujen kehitystä

2.2.2 järjestelmäpäivityksiä, konfiguraatioiden testausta ja integraatiotestausta

2.2.3 automatisoituja ja manuaalisia toiminnallisia testejä tai tietoturvatestejä

3. Tavoitteet

3.1 Estää aidon, tunnistettavan asiakasdatan käyttö testauksessa, ellei dataa ole anonymisoitu ja käytölle ole annettu nimenomaista hyväksyntää.

3.2 Ylläpitää testi- ja tuotantoympäristöjen tiukka erottelu tahattoman tietojen altistumisen tai toiminnallisten häiriöiden välttämiseksi.

3.3 Suojata testijärjestelmät ja testidata luvattomalta pääsyltä, tahattomalta paljastumiselta tai uudelleenkäytöltä eri ympäristöissä ilman asianmukaisesti toteutettuja kontrolleja.

3.4 Noudattaa sovellettavia tietosuojavaatimuksia (esim. GDPR, NIS2) varmistamalla, että kaikkea testidataa käsitellään lainmukaisesti, asianmukaisesti ja turvallisesti.

3.5 Tukea organisaation valmiutta ulkoisiin auditointeihin ja ISO/IEC 27001 -sertifiointiin dokumentoimalla testauskäytännöt ja varmistamalla yhdenmukaisten suojatoimien toteuttaminen.

4. Roolit ja vastuut

4.1 Toimitusjohtaja

4.1.1 Vastaa kokonaisuutena testidatan suojaamisesta ja testijärjestelmien tietoturvasta.

4.1.2 Hyväksyy aidon datan käytön testauksessa varmistuttuaan siitä, että asianmukaiset suojatoimet (esim. anonymisointi tai tietojen maskaus) on toteutettu.

4.1.3 Varmistaa, että testaustoiminta dokumentoidaan asianmukaisesti ja että se noudattaa tätä politiikkaa.

4.2 Projektin omistaja

4.2.1 Koordinoi testausprosessien suunnittelua ja toteutusta.

4.2.2 Varmistaa, että kaikki tiimin jäsenet ymmärtävät tämän politiikan ja noudattavat sitä.

4.2.3 Vahvistaa ennen testauksen aloittamista, että testijärjestelmät on konfiguroitu turvallisesti.

4.2.4 Ilmoittaa toimitusjohtajalle kaikista testiympäristöihin tai tietojen altistumiseen liittyvistä poikkeamista.

[... Jaksot 4.3–8 eivät sisälly tähän esikatseluun. Osta koko asiakirja saadaksesi täyden sisällön. ...]

9. Katselmointi- ja päivitysvaatimukset

9.1 Säännölliset katselmoinnit

9.1.1 Toimitusjohtajan on katselmoitava tämä politiikka vähintään kerran vuodessa. Katselmoinnilla varmistetaan, että politiikka pysyy ajan tasalla seuraavien osalta:

9.1.1.1 ohjelmistokehityksen työkalujen, alustojen tai ympäristöjen muutokset

9.1.1.2 päivitetyt oikeudelliset velvoitteet, mukaan lukien tietosuojaa tai digitaalista häiriönsietokykyä koskevat vaatimukset

9.1.1.3 pk-yrityksen ISO/IEC 27001 -sertifiointiin liittyvä auditointivalmius

9.2 Välikatselmoinnin käynnistävät tapahtumat

9.2.1 Lisäkatselmointeja on tehtävä seuraavien tapahtumien jälkeen:

9.2.1.1 mikä tahansa testiympäristössä tapahtunut tietojen altistuminen tai vaarantuminen

9.2.1.2 aidon datan käyttö testauksessa, vaikka data olisi anonymisoitu

9.2.1.3 uusien testausmenetelmien, järjestelmien tai toimittajien käyttöönotto

9.2.1.4 sääntelymuutokset, jotka vaikuttavat tietojen käsittelyyn testauksen aikana

9.3 Muutoksenhallinta ja viestintä

9.3.1 Toimitusjohtaja vastaa seuraavista:

9.3.1.1 tämän politiikan päivittämisestä ja kaikkien muutosten dokumentoinnista versiohistorian avulla

9.3.1.2 henkilöstön, kehittäjien ja asiaankuuluvien palveluntarjoajien tiedottamisesta päivityksistä

9.3.1.3 sen varmistamisesta, että kaikki testaukseen liittyvät henkilöt ymmärtävät ja soveltavat uusimpia vaatimuksia

9.3.1.4 uusimman politiikkaversion pitämisestä saatavilla katselmointi- ja auditointitarkoituksia varten

9.4 Auditointi ja dokumentaatio

9.4.1 Tallenteet kaikista politiikan katselmoinneista, aidon datan käytön hyväksynnöistä ja poikkeusten perusteluista on:

9.4.1.1 säilytettävä turvallisesti auditointitarkoituksia varten

9.4.1.2 oltava saatavilla pyynnöstä sisäisten tai kolmannen osapuolen auditointien yhteydessä

9.4.1.3 katselmoitava vuosittain sen varmistamiseksi, että ne ovat yhdenmukaisia testauskäytäntöjen kanssa

10. Liittyvät politiikat ja yhteydet

10.1 Tätä politiikkaa on sovellettava yhdessä seuraavien pk-yrityksen politiikkojen kanssa tietoturvan ja vaatimustenmukaisuuden varmistamiseksi testauksen aikana:

10.1.1 P2S – Hallintoroolit ja -vastuut -politiikka: määrittää, kuka vastaa kehityksen, testauksen ja järjestelmien erotteluun liittyvien vastuiden valvonnasta.

10.1.2 P4S – Pääsynhallintapolitiikka: ohjaa testijärjestelmien tunnistetietojen myöntämistä, hallintaa ja poistamista.

10.1.3 P8S – Tietoturvatietoisuus- ja koulutuspolitiikka: varmistaa, että henkilöstö ymmärtää testidataan liittyvät riskit, turvalliset käsittelykäytännöt ja ympäristöjen asianmukaisen erottelun.

10.1.4 P13S – Tiedon luokittelu- ja merkintäpolitiikka: tukee testidatan selkeää luokittelua ja ohjaa anonymisointi- tai tietojen maskausstrategioita.

10.1.5 P17S – Tietosuoja- ja yksityisyydensuojapolitiikka: varmistaa yhdenmukaisuuden GDPR-velvoitteiden kanssa, mukaan lukien henkilötietojen käsittelyyn ja tallentamiseen liittyvät suojatoimet myös testiympäristöissä.

10.1.6 P24S – Turvallisen kehittämisen politiikka: määrittää kehitystiimeille yleiset tietoturvavaatimukset, mukaan lukien datan turvallinen käyttö testausvaiheissa.

10.1.7 P30S – Tietoturvapoikkeamien hallintapolitiikka: kuvaa toimintatavan tilanteissa, joissa testiympäristössä havaitaan tietoturvaloukkaus tai muu ongelma tai jotka johtuvat testidatan epäasianmukaisesta käsittelystä.

10.2 Nämä politiikat muodostavat yhtenäisen tietoturvan viitekehyksen, joka tukee testauksen eheyttä, tietojen minimointia ja ISO/IEC 27001 -vaatimusten mukaista toimintaa koko kehitys- ja laadunvarmistustoiminnassa.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Kohta 6.1 – edellyttää riskien arviointia ja riskien käsittelytoimia, mukaan lukien testaukseen liittyvät riskit.

11.1.2 Kohta 8.1 – edellyttää operatiivisten prosessien suunnittelua ja hallintaa, mukaan lukien testijärjestelmien käyttöön liittyvät ympäristöt.

11.2 ISO/IEC 27002

11.2.1 Kontrolli 8.28 – edellyttää, että organisaatiot suojaavat testidataa ja varmistavat, ettei se sisällä arkaluonteista tai tuotannossa käytettävää aitoa dataa.

11.2.2 Kontrolli 8.29 – edellyttää kehitys-, testi- ja tuotantoympäristöjen selkeää erottamista toisistaan.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – kattaa kehitykseen ja testaukseen liittyvät kontrollivaatimukset.

11.3.2 SA-12 – käsittelee toimitusketjun testausriskejä ja tietoturva-arviointeja.

11.3.3 SC-32 – edellyttää ympäristöjen erottamista sekä testidatan luottamuksellisuuden ja eheyden suojaamista.

11.4 EU:n yleinen tietosuoja-asetus (GDPR)

11.4.1 Artikla 5(1)(c) – edellyttää tietojen minimointia, mukaan lukien vain tarpeellisten tietojen käyttö testauksessa.

11.4.2 Artikla 25 – edellyttää sisäänrakennettua ja oletusarvoista tietosuojaa, johon sisältyvät myös testiympäristöjen hallintatoimet.

11.4.3 Artikla 32 – edellyttää henkilötietojen turvallista käsittelyä kaikissa järjestelmissä, mukaan lukien ei-tuotantoympäristöt.

11.5 EU:n NIS2-direktiivi (2022/2555)

11.5.1 Artikla 21(2)(e, h) – edellyttää turvallista kehittämistä ja järjestelmätestausta erityisesti silloin, kun digitaaliset palvelut altistuvat kyberriskeille.

11.6 EU:n DORA-asetus (2022/2554)

11.6.1 Artikla 9 – korostaa digitaalisen operatiivisen häiriönsietokyvyn merkitystä, mukaan lukien ICT-järjestelmien turvallinen testaus finanssialan pk-yrityksissä.

11.7 COBIT 2019

11.7.1 BAI07 – Muutosten hyväksynnän ja siirtymien hallinta: sisältää testauskontrolleja uusien järjestelmien ja tietojen käsittelyn validointiin.

11.7.2 DSS05 – Tietoturvapalvelujen hallinta: edellyttää testaus- ja kehityskäytäntöjä, jotka estävät liiketoimintadatan väärinkäytön tai altistumisen.