					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P29					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	Kohta 8	Liittyy testidatan ja testiympäristöjen turvalliseen suunnitteluun ja hallintaan
ISO/IEC 27002:2022	Kontrollit 8.28–8.29	Kattaa testidatan turvallisen käsittelyn ja testiympäristöjen suojauksen
NIST SP 800-53 Rev.5	SA-11, SC-28, SC-32	Käsittelee kehittäjien testausta ja arviointia, lepotilassa olevien tietojen suojausta sekä tietojen eheyttä
EU:n GDPR	Artiklat 5, 25, 32	Kattaa tietojen minimoinnin, sisäänrakennetun tietosuojan ja käsittelyn turvallisuuden testauskontekstissa
EU:n NIS2-direktiivi	Artikla 21(2)(e), (h)	Liittyy turvallisiin kehitys- ja testauskäytäntöihin
EU:n DORA-asetus	Artikla 9	Koskee ICT-järjestelmiä ja -protokollia sekä testidatan turvallisuutta
COBIT 2019	DSS05, BAI07	Käsittelee tietoturvapalvelujen hallintaa sekä muutosten hyväksyntää ja siirtymää

1. Tarkoitus

1.1. Tämä politiikka määrittää pakolliset vaatimukset testiympäristöjen ja testidatan hallinnalle turvallisuuden, luottamuksellisuuden ja toiminnallisen eheyden varmistamiseksi koko ohjelmistokehityksen ja testauksen elinkaaren ajan.

1.2. Politiikan tavoitteena on estää luvaton pääsy, tietovuodot ja tuotantojärjestelmien kontaminoituminen puutteellisesti hallittujen testiympäristöjen tai testauksessa käytetyn todellisen tuotantodatan seurauksena.

1.3. Tämä politiikka edellyttää testauksessa käytettävien tietojen turvallista käsittelyä, testiinfrastruktuurin koventamista ja roolipohjaista käyttöoikeuksien hallintaa sekä varmistaa yhdenmukaisuuden sovellettavien sääntely- ja sopimusvelvoitteiden kanssa.

2. Soveltamisala

2.1. Tämä politiikka koskee kaikkia organisaatiossa ohjelmistojen, järjestelmien, sovellusten ja infrastruktuurin testaukseen käytettäviä testiympäristöjä, tietoja, työkaluja ja prosesseja.

2.2. Politiikka kattaa seuraavat:

2.2.1. Testiympäristöt, jotka on provisioitu omissa tiloissa, pilviympäristössä tai kolmannen osapuolen alustoilla

2.2.2. Testidata, jota käytetään toiminnallisessa testauksessa, suorituskykytestauksessa, regressiotestauksessa ja tietoturvatestauksessa

2.2.3. Manuaalinen, skriptipohjainen tai automatisoitu testaus (esim. CI/CD-putket)

2.2.4. Kaikki testaukseen osallistuvat henkilöt, mukaan lukien sisäiset tiimit, toimittajat ja urakoitsijat

2.3. Tätä politiikkaa sovelletaan riippumatta järjestelmän kriittisyydestä, sovellustyypistä tai siitä, toteutetaanko kehitys sisäisesti vai ulkoistettuna.

3. Tavoitteet

3.1. Estää tuotantodatan, arkaluonteisten tietojen tai sääntelyn alaisten tietojen (esim. henkilötiedot, maksukorttitiedot) käyttö testiympäristöissä, ellei tietoja ole anonymisoitu tai käyttöä ole nimenomaisesti hyväksytty.

3.2. Varmistaa testaus- ja tuotantoympäristöjen täydellinen erottelu verkkojen ja pääsynhallinnan osalta luvattoman tietojen käytön tai järjestelmien kontaminoitumisen estämiseksi.

3.3. Edellyttää salausta, tietojen maskausta tai synteettisen datan tuottamista, kun testaukseen tarvitaan edustavaa dataa.

3.4. Vähentää vaatimustenvastaisuuden, asiakastietojen altistumisen tai toiminnan häiriöiden todennäköisyyttä, jotka johtuvat turvattomasta testidatasta tai testiympäristöistä.

3.5. Varmistaa, että testidatan käsittely on yhdenmukainen toimialan standardien (ISO, NIST, COBIT) sekä sääntelyn, kuten EU:n GDPR:n, EU:n NIS2-direktiivin ja EU:n DORA-asetuksen, kanssa.

4. Roolit ja vastuut

4.1. Tietoturvajohtaja (CISO)

4.1.1. Omistaa tämän politiikan ja varmistaa teknisten ja hallinnollisten suojatoimien toteutuksen testidataa ja testiympäristöjä varten.

4.1.2. Hyväksyy todellisen tai arkaluonteisen datan käytön testauksessa asianmukaisen perustelun ja korvaavien kontrollien perusteella.

4.2. QA-/testausvastaavat

4.2.1. Koordinoivat testauksen suunnittelua ja varmistavat, että kaikki testaustoiminnot noudattavat tämän politiikan vaatimuksia.

4.2.2. Varmistavat asianmukaisen eriyttämisen, käyttöoikeudet ja datan valmistelun jokaisessa testausvaiheessa.

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

9. Katselmointi- ja päivitysvaatimukset

9.1. Tämä politiikka on katselmoitava vuosittain ja päivitettävä tarvittaessa seuraavien muutosten huomioimiseksi:

9.1.1. Muutokset sääntelyvaatimuksissa (esim. EU:n GDPR, EU:n DORA-asetus, EU:n NIS2-direktiivi)

9.1.2. Uusien testaustyökalujen, alustojen tai automaatioputkien käyttöönotto

9.1.3. Sisäisen tarkastuksen auditointihavainnot tai poikkeaman jälkeiset suositukset

9.1.4. Kehitys- tai QA-prosessien laajentuminen, joka muuttaa testidatan käsittelyä tai ympäristöjen käyttöä

9.2. Tietoturvajohtaja (CISO) vastaa katselmoinnin käynnistämisestä yhteistyössä seuraavien kanssa:

9.2.1. QA-/testausvastaavat

9.2.2. DevOps- ja infrastruktuuripäälliköt

9.2.3. Sovelluskehitystiimit

9.2.4. Tietosuojavastaava ja oikeudellinen neuvonantaja

9.3. Kaikkien muutosten on oltava:

9.3.1. versiohallittuja ja tallennettu keskitettyyn dokumenttirekisteriin

9.3.2. viestitty asianomaiselle henkilöstölle muodollisten kanavien kautta (esim. ISMS-ilmoitukset, tiimitiedotukset)

9.3.3. yhdistetty niihin liittyvien teknisten standardien, kontrollien ja toimintaohjeiden päivityksiin

9.4. Heräteperusteiset väliaikaiset katselmoinnit on tehtävä välittömästi seuraavien jälkeen:

9.4.1. Testiympäristöihin liittyvä tietovuoto tai tietomurto

9.4.2. Testidatan käsittelyyn liittyvä auditointipoikkeama

9.4.3. Merkittävät muutokset oikeudellisissa velvoitteissa tai IT-arkkitehtuurissa

10. Liittyvät politiikat ja yhteydet

10.1. Tämä politiikka liittyy kiinteästi seuraaviin politiikkoihin testidatan ja testiympäristöjen turvallisen ja vaatimustenmukaisen käsittelyn varmistamiseksi:

10.1.1. P1 – Tietoturvapolitiikka: Määrittää yleiset tietoturvaperiaatteet, jotka ohjaavat testidatan suojausta ja ympäristöjen hallintaa.

10.1.2. P5 – Muutoksenhallintapolitiikka: Sovelletaan testiympäristöjen luomiseen, päivittämiseen ja käytöstä poistoon sekä käyttöönottoputkiin.

10.1.3. P13 – Tiedon luokittelu- ja merkintäpolitiikka: Ohjaa testidatan valintaa ja arkaluonteisuuteen perustuvien kontrollien toteutusta.

10.1.4. P14 – Tietojen säilytys- ja hävityspolitiikka: Määrittää testitietoaineistojen säilytysajat ja turvallista hävittämistä koskevat vaatimukset.

10.1.5. P15 – Varmuuskopiointi- ja palautuspolitiikka: Edellyttää varmuuskopiointikäytäntöjä ja palautuksen validointia testiympäristöille.

10.1.6. P18 – Kryptografisten hallintakeinojen politiikka: Määrittää pakolliset salausstandardit testialustoilla oleville lepotilassa oleville tiedoille ja siirrettäville tiedoille.

10.1.7. P22 – Lokitus- ja valvontapolitiikka: Ohjaa näkyvyyttä ja poikkeamien havaitsemista testiympäristöjen toiminnassa.

10.1.8. P30 – Tietoturvapoikkeamien hallintapolitiikka: Määrittää testijärjestelmiin liittyvien tietomurtojen ja poikkeamien eskaloinnin ja korjaavat toimenpiteet.

10.1.9. P33 – Auditointi- ja vaatimustenmukaisuuden seurantapolitiikka: Mahdollistaa politiikan noudattamisen varmentamisen ja jatkuvan varmistamisen.

11. Viitestandardit ja viitekehykset

11.1. Tämä politiikka on yhdenmukainen kansainvälisten kyberturvallisuusstandardien ja sääntelyviitekehysten kanssa, jotka edellyttävät testidatan turvallista käsittelyä ja ei-tuotantoympäristöjen suojaamista.

11.2. ISO/IEC 27001:

11.2.1. Kohta 8.1 – Edellyttää testidatan ja testiympäristöjen turvallista suunnittelua ja hallintaa.

11.3. ISO/IEC 27002:2022 – Kontrollit 8.28–8.29:

11.3.1. Liite A, kontrolli 8.28 – turvallinen testidata: Edellyttää kehitys- ja testausvaiheissa käytettävän testidatan suojaamista anonymisoinnin, maskauksen tai synteettisen datan tuottamisen avulla.

11.3.2. Liite A, kontrolli 8.29 – testiympäristöjen suojaus: Edellyttää testijärjestelmien erottelua tuotannosta, pääsynhallintaa ja ympäristön koventamista.

11.3.3. Nämä kontrollit määrittävät vaatimukset testauksen aikana käytettävien tietojen turvalliselle hallinnalle sekä ei-tuotantojärjestelmien suojaamiselle väärinkäytöltä, vaarantumiselta tai kontaminoitumiselta.

11.4. NIST SP 800-53 Rev.5:

11.4.1. SA-11 – Kehittäjän testaus ja arviointi: Määrittää odotukset turvallisille, toistettaville testausmenettelyille asianmukaisine datakontrolleineen.

11.4.2. SC-28 – Lepotilassa olevien tietojen suojaus: Vastaa ei-tuotantojärjestelmiin tallennetun testidatan salausta.

11.4.3. SC-32 – Tietojen eheys: Tukee datan validointia, korruptoitumisen estämistä sekä syöte- ja tulostekontrolleja testauksen aikana.

11.5. EU:n GDPR (2016/679):

11.5.1. Artikla 5 – tietojen minimointi: Kieltää henkilötietojen tarpeettoman käytön testauksessa.

11.5.2. Artikla 25 – sisäänrakennettu tietosuoja: Edellyttää tietosuojatekniikoiden soveltamista kehitys- ja testausjakson alusta lähtien.

11.5.3. Artikla 32 – käsittelyn turvallisuus: Edellyttää suojatoimia testiympäristöille, joissa käsitellään henkilötietoja tai arkaluonteisia tietoja.

11.6. EU:n NIS2-direktiivi (2022/2555):

11.6.1. Artikla 21(2)(e, h): Edellyttää turvallisia ohjelmistokehityksen ja testauksen prosesseja painottaen suojaa luvatonta pääsyä ja tietovuotoja vastaan.

11.7. EU:n DORA-asetus (2022/2554):

11.7.1. Artikla 9 – ICT-järjestelmät ja -protokollat: Edellyttää, että testausprosessit tukevat häiriönsietokykyä ja suojaavat operatiivisia tietoja vaarantumiselta tai luvattomalta paljastumiselta.

11.8. COBIT 2019:

11.8.1. DSS05 – Tietoturvapalvelujen hallinta: Tukee tietoturvapolitiikkojen soveltamista kaikissa ympäristöissä, mukaan lukien ei-tuotantoympäristöt.

11.8.2. BAI07 – Muutosten hyväksynnän ja siirtymän hallinta: Kattaa muodollisen siirtymäprosessin testauksesta tuotantoon, mukaan lukien dataa ja ympäristöjä koskevat kontrollit.