| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Lisää tähän rekisteröidyn oikeushenkilön nimi | | | | | | | |
| Asiakirjan numero:<br>P24 | | | | | Asiakirjan nimi:<br>**Turvallisen kehityksen politiikka** | | | | | | | |
| Versio:<br>1.0 | | Voimaantulopäivä:<br>01.01.2025 | | | Asiakirjan omistaja: | | | | | | | |
| X | Politiikka | | Standardi | | Menettely | | Lomake | | Rekisteri | | Muu | |

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

| **Hyväksynnät** | | | |
|---|---|---|---|
| **Nimi** | **Tehtävänimike** | **Päivämäärä** | **Allekirjoitus** |
| | | | |
| | | | |

## 1. Tarkoitus

1.1 Tämä politiikka määrittää pakolliset tietoturvavaatimukset organisaation ohjelmisto- ja järjestelmäkehitykselle, mukaan lukien sisäiset projektit, ulkoistettu kehitys ja kolmannen osapuolen koodin integrointi.

1.2 Tavoitteena on varmistaa, että tietoturva sisällytetään koko ohjelmistokehityksen elinkaareen (SDLC) ja että haavoittuvuudet tunnistetaan, lievennetään ja estetään ennen käyttöönottoa tuotantoympäristöön.

1.3 Tämä politiikka tukee ISO/IEC 27001:2022 -standardin lausekkeen 8.1 ja liitteen A kontrollien 8.25–8.28 soveltamista standardoimalla turvallisen kehityksen hallintaa, koodin validointikäytäntöjä ja kolmannen osapuolen kehityksen valvontaa.

## 2. Soveltamisala

### 2.1 Tämä politiikka koskee kaikkia seuraavia:

2.1.1 Sisäisesti tai ulkoisesti kehitettyjä ohjelmistoja, sovelluksia, skriptejä, integraatioita ja automaatiotyökaluja

2.1.2 Kehitystiimejä, tuoteomistajia, DevOps-toimintoja, laadunvarmistustoimintoja, arkkitehteja, projektipäälliköitä ja sopimuskumppaneita

2.1.3 SDLC-ympäristöjä, mukaan lukien kehitys-, testaus-, vaiheistus- ja esituotantoympäristöt

2.1.4 Sisäisiin sovelluksiin integroituja avoimen lähdekoodin ja kolmannen osapuolen komponentteja

2.1.5 Ohjelmistoja, jotka on otettu käyttöön omissa tiloissa, yksityisessä pilviympäristössä, hybridiympäristössä tai julkisessa pilviympäristössä

2.2 Kaikki käyttäjät ja osapuolet, jotka osallistuvat järjestelmien kehitykseen, testaukseen tai käyttöönottoon organisaation toimintaympäristössä, kuuluvat tämän politiikan soveltamisalaan, mukaan lukien hallinnoidut palveluntarjoajat (MSP) ja alustatoimittajat.

## 3. Tavoitteet

3.1 Sisällyttää tietoturvakontrollit ohjelmistokehityksen kaikkiin vaiheisiin suunnittelusta käyttöönottoon siten, että riskien vähentäminen on ennakoivaa ja jatkuvaa.

3.2 Estää hyväksikäytettävissä olevien haavoittuvuuksien syntyminen, kuten injektiohaavoittuvuudet, epävarma todennus ja altistuminen tunnetuille kolmannen osapuolen heikkouksille.

3.3 Määrittää ja soveltaa turvallisen ohjelmoinnin käytäntöjä OWASP:n, SANS CWE:n ja viitekehyskohtaisten ohjeiden mukaisesti.

3.4 Varmistaa, että kaikki koodi käy läpi vertaiskatselmoinnin, automatisoidun analyysin ja tietoturvavalidoinnin ennen käyttöönottoa.

3.5 Hallita kehitysriskejä, jotka johtuvat ulkoistetuista toiminnoista, kolmannen osapuolen koodin sisällyttämisestä ja avoimen lähdekoodin ohjelmistojen uudelleenkäytöstä.

3.6 Suojata kehitys-, testaus- ja vaiheistusympäristöt luvattomalta pääsyltä ja estää tuotantodatan käyttö ilman hyväksyttyä tietojen maskausta tai anonymisointia.

3.7 Edistää kehittäjien, tuotepäälliköiden ja laadunvarmistuksen ammattilaisten tietoturvatietoisuutta roolipohjaisen koulutuksen ja esiin nousevia uhkia koskevien jatkuvien päivitysten avulla.

## 4. Roolit ja vastuut

### 4.1 Tietoturvajohtaja (CISO)

4.1.1 Omistaa tämän politiikan ja varmistaa, että turvallisen kehityksen vaatimuksia sovelletaan koko organisaatiossa.

4.1.2 Hyväksyy turvallisen ohjelmoinnin standardit ja kolmannen osapuolen kehitystä koskevat sopimusvaatimukset.

4.1.3 Vahvistaa riskienkäsittelyä koskevat päätökset ratkaisemattomien tai lykättyjen haavoittuvuuksien osalta.

**4.2 Sovellustietoturvasta vastaava henkilö / DevSecOps-päällikkö**

4.2.1 Laatii, ylläpitää ja edistää turvallisen ohjelmoinnin ohjeita.

4.2.2 Integroi staattisen ja dynaamisen tietoturvatestauksen CI/CD-putkiin.

4.2.3 Suorittaa koodin tietoturvakatselmointeja ja määrittää pakolliset korjaavat toimenpiteet.

[ ... 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 tai useammin seuraavien muutosten perusteella:**

9.1.1 Merkittävät muutokset kehitysmenetelmissä tai DevOps-työkaluissa

9.1.2 Olennaiset tietoturvapoikkeamat, jotka johtuvat sovellushaavoittuvuuksista

9.1.3 Muutokset turvallisia ohjelmistoja koskevissa sääntelyvaatimuksissa (esim. EU:n GDPR, DORA-asetus)

9.1.4 Uudet toimialastandardit tai uhkatiedustelu (esim. OWASP Top 10, SLSA, MITRE CWE)

9.2 Politiikan katselmoinnista vastaa sovellustietoturvasta vastaava henkilö yhteistyössä tietoturvajohtajan (CISO), ohjelmistoarkkitehtien, laadunvarmistusjohdon ja oikeudellisen neuvonnan kanssa (kolmannen osapuolen koodiin liittyvien vaikutusten osalta).

9.3 Kaikki muutokset on kirjattava ISMS:n asiakirjahallintarekisteriin, pidettävä versiohallittuina ja viestittävä vaikutuksen piirissä oleville tiimeille julkaisutiedotteilla tai pakollisella koulutuksella.

9.4 Perintöversiot on säilytettävä arkistotietovarastossa oikeudellisen jäljitettävyyden ja auditointijäljen varmistamiseksi.

**10. Liittyvät politiikat ja yhteydet**

10.1 P1 – Tietoturvapolitiikka. Määrittää strategisen vaatimuksen tietoturvan sisällyttämisestä kaikkiin tietojärjestelmiin, joista turvallinen kehitys on keskeinen operatiivinen kontrolli.

10.2 P4 – Pääsynhallintapolitiikka. Määrittää kontrollit kehitysympäristöjen, tietovarastojen, build-työkalujen ja CI/CD-putkien käyttöoikeuksien rajoittamiseksi.

10.3 P5 – Muutoksenhallintapolitiikka. Varmistaa, että koodimuutokset, julkaisut ja käyttöönotot ovat asianmukaisen hyväksynnän, palautussuunnittelun ja käyttöönoton jälkeisen varmistuksen piirissä.

10.4 P12 – Omaisuudenhallintapolitiikka. Tukee kehitysympäristöjen, lähdekooditietovarastojen ja build-järjestelmien ylläpitämistä hallittuina omaisuuserinä, joihin sovelletaan luokittelua ja suojausta.

10.5 P22 – Lokitus- ja valvontapolitiikka. Soveltuu kehitysputkiin ja varmistaa, että build-prosessit, koodin siirrot ja käyttöönottoon liittyvät tapahtumat lokitetaan, niitä valvotaan ja analysoidaan tietoturvapoikkeamien varalta.

10.6 P30 – Tietoturvapoikkeamien hallintapolitiikka. Tarjoaa viitekehyksen käyttöönoton jälkeen tai sovellustietoturvatestauksen aikana havaittujen tietoturvapuutteiden analysointiin ja käsittelyyn.

**11. Viitestandardit ja viitekehykset**

**11.1 ISO/IEC 27001**

11.1.1 Lauseke 8.1 – Toiminnan suunnittelu ja ohjaus: edellyttää turvallisten kehitysprosessien ja kontrollien integrointia operatiiviseen toimintaan.

**11.2 ISO/IEC 27002:2022 – Kontrollit 8.25–8.28**

11.2.1 Liitteen A kontrolli 8.25 – Turvallinen kehityksen elinkaari: edellyttää tietoturvan muodollista sisällyttämistä ohjelmistojen suunnitteluun ja kehitykseen.

11.2.2 Liitteen A kontrolli 8.26 – Sovellusten tietoturvavaatimukset: edellyttää turvallisen ohjelmoinnin ja tietoturvan hyväksymiskriteerien määrittelyä.

11.2.3 Liitteen A kontrolli 8.27 – Turvallinen järjestelmäarkkitehtuuri ja suunnitteluperiaatteet: edellyttää tietoturvasuunnittelun periaatteiden soveltamista ja tunnettujen heikkouksien lieventämistä.

11.2.4 Liitteen A kontrolli 8.28 – Turvallinen ohjelmointi: edellyttää turvallisen ohjelmoinnin periaatteiden soveltamista.

**11.3 NIST SP 800-53 Rev. 5**

11.3.1 SA-3–SA-15: määrittää jäsennellyt sovellustietoturvan kehityskäytännöt, mukaan lukien suunnittelua, koodin eheyttä ja testausta koskevat vaatimukset.

11.3.2 SI-10 – Tiedonsyötteen validointi: koskee turvallisen ohjelmoinnin suojatoimia.

11.3.3 SR-3 – Toimitusketjun suojaus: edellyttää kolmannen osapuolen ohjelmistojen, komponenttien ja kehityspalveluntarjoajien arviointia.

**11.4 EU:n GDPR (2016/679)**

11.4.1 Artikla 25 – Sisäänrakennettu ja oletusarvoinen tietosuoja: edellyttää tietoturvan ja tietosuojan sisällyttämistä järjestelmäkehitykseen.

11.4.2 Artikla 32 – Käsittelyn turvallisuus: tukee teknisiä toimenpiteitä, kuten syötteiden validointia, pääsynhallintaa ja turvallista käyttöönottoa.

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

11.5.1 Artikla 21(2)(e–f): edellyttää ohjelmistokehityskäytäntöjä, joihin sisältyvät haavoittuvuuksien hallinta, koodin tietoturva ja poikkeamien ilmoittaminen.

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

11.6.1 Artikla 9 – ICT-riskien hallinta: edellyttää turvallisen kehityksen käytäntöjä finanssialan toimijoille, mukaan lukien ohjelmistojen laadun kontrollit ja puutteiden korjaaminen.

11.6.2 Artikla 10 – Liiketoiminnan jatkuvuus ja testaus: edellyttää ICT-järjestelmien, mukaan lukien sovellusten, perusteellista testausta ja validointia.

**11.7 COBIT 2019**

11.7.1 BAI03 – Ratkaisujen tunnistamisen ja toteutuksen hallinta: ohjaa suunnittelua, kehitystä ja tietoturvan integrointia uusiin ratkaisuihin.

11.7.2 BAI07 – Muutosten hyväksynnän ja siirtymien hallinta: varmistaa turvallisen käyttöönoton ja käyttöönoton jälkeisen arvioinnin.

11.7.3 DSS05 – Tietoturvapalveluiden hallinta: soveltaa tietoturvavalidointia ohjelmistojen ja palveluiden tuottamiseen.