					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P24S					Asiakirjan nimi: **Turvallisen kehityksen 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	Merkitykselliset tietoturvakontrollit operatiivisiin käytäntöihin, mukaan lukien turvallinen kehitys
ISO/IEC 27002:2022	Kontrollit 8.25–8.27	Kattaa turvallisen järjestelmäkehityksen elinkaaren, testauksen sekä kolmannen osapuolen kehittäjien tietoturvavelvoitteet
NIST SP 800-53 Rev.5	SA-3 – SA-15, SI-10	Käsittelee turvallista ohjelmistokehityksen elinkaarta, pääsynhallintaa ja haavoittuvuuksien käsittelyä kehityksessä
EU:n GDPR	Artikla 25	Edellyttää sisäänrakennettua ja oletusarvoista tietosuojaa ohjelmistokehityksessä
EU:n NIS2-direktiivi	Artikla 21(2)(a), (e), (h)	Velvoittaa turvallisen kehityksen politiikkoihin, avoimen lähdekoodin käytön valvontaan ja lieventämistoimenpiteiden dokumentointiin
EU:n DORA-asetus	Artiklat 6(7), 9(1)(c), 10(2)(c)	Elinkaaren aikainen tietoturva rahoitussektorin kriittisille ICT-järjestelmille
COBIT 2019	BAI	Viitekehys jäsenneltyyn, jäljitettävään ja häiriönsietokykyiseen turvallisen kehityksen hallintaan

1. Tarkoitus

1.1 Tämän politiikan tarkoituksena on varmistaa, että kaikki organisaation tai sen ulkoisten kumppaneiden luomat tai muokkaamat ohjelmistot, skriptit ja verkkopohjaiset työkalut kehitetään turvallisesti siten, että haavoittuvuuksien, luvattoman tiedonsaannin ja toimintahäiriöiden riski minimoidaan.

1.2 Tässä politiikassa määritellään pakolliset turvallisen kehityksen säännöt ja turvallisen ohjelmoinnin käytännöt, joita kaikkien sisäisten kehittäjien, sopimuskumppaneiden ja toimittajien on noudatettava projektin koosta tai monimutkaisuudesta riippumatta.

1.3 Tämän politiikan tarkoituksena on suojata asiakastietoja, ehkäistä tietomurtoja sekä varmistaa, että organisaation toteuttamat tai organisaatiolle räätälöidyt ohjelmistot ovat tietoturvan näkökulmasta auditoitavissa, täyttävät lakisääteiset vaatimukset (esim. EU:n GDPR, EU:n NIS2-direktiivi, EU:n DORA-asetus) ja tukevat ISO/IEC 27001 -sertifiointia.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia henkilöitä ja tahoja, jotka organisaation puolesta kehittävät, räätälöivät, ottavat käyttöön tai hallinnoivat seuraavia:

2.1.1 Verkkosivustoja, sovelluksia tai automaatiotyökaluja

2.1.2 Sisäisesti kehitettyjä skriptejä tai ohjelmistoja

2.1.3 Kolmannen osapuolen kehittäjien tai freelancerien tuottamaa koodia

2.1.4 Liitännäisiä, kirjastoja ja ohjelmistokomponentteja, jotka integroidaan tuotantojärjestelmiin

2.2 Politiikka kattaa kaikki kehitystoiminnassa käytettävät ympäristöt, mukaan lukien:

2.2.1 Kehitys- ja testausympäristöt

2.2.2 Vaiheistus- ja esituotantoympäristöt

2.2.3 Tuotantojärjestelmät, joissa suoritetaan räätälöityä koodia

2.3 Politiikka ohjaa myös tietojen käsittelyä kehityksen ja käyttöönoton aikana, erityisesti tuotantotietojen käyttöä ei-tuotantoympäristöissä.

3. Tavoitteet

3.1 Estää tietoturvavirheiden tai haavoittuvuuksien syntyminen räätälöidyissä ohjelmistoissa tai kolmannen osapuolen kehittämissä ohjelmistoissa.

3.2 Varmistaa, että turvallisen ohjelmoinnin käytännöt ja haavoittuvuuksien ehkäisy integroidaan ohjelmistokehityksen elinkaaren jokaiseen vaiheeseen.

3.3 Vähentää avoimen lähdekoodin tai kolmannen osapuolen komponenttien käyttöön liittyviä riskejä edellyttämällä asianmukaista arviointia ja seurantaa.

3.4 Edellyttää muodollista koodikatselmointia ja sovellustietoturvatestausta ennen julkaisua.

3.5 Hallita pääsyä kehitysympäristöihin ja varmistaa niiden erottaminen tuotantojärjestelmistä.

3.6 Täyttää kansainvälisten standardien ja sääntelyn pakolliset vaatimukset (esim. ISO/IEC 27001, EU:n GDPR, EU:n DORA-asetus, EU:n NIS2-direktiivi).

4. Roolit ja vastuut

4.1 Toimitusjohtaja (GM)

4.1.1 Hyväksyy tämän politiikan ja vastaa siitä.

4.1.2 Varmistaa, että kaikki ohjelmistokehitys, riippumatta siitä onko se sisäistä vai ulkoistettua, noudattaa tätä politiikkaa.

4.1.3 Katselmoi ja allekirjoittaa kehitys- tai palvelusopimukset, jotka sisältävät turvallista kehitystä koskevat ehdot.

4.1.4 Varmistaa toimittajien vaatimustenmukaisuuden säännöllisillä katselmoinneilla tai pyytämällä tietoturvaa koskevaa näyttöä.

4.2 Sisäinen kehittäjä tai sovellusomistaja

4.2.1 Noudattaa turvallisen ohjelmoinnin käytäntöjä ja käyttöönottomenettelyjä.

4.2.2 Soveltaa turvallisen kehityksen tarkistuslistaa jokaisessa projektissa.

4.2.3 Varmistaa kaikkien käytettävien avoimen lähdekoodin tai kolmannen osapuolen komponenttien tietoturvan.

4.2.4 Ilmoittaa kaikista havaituista haavoittuvuuksista toimitusjohtajalle (GM) välittömästi.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Toimitusjohtajan on katselmoitava tämä politiikka vähintään kerran vuodessa seuraavia tarkoituksia varten:

9.1.1 Varmistaa jatkuva yhdenmukaisuus ISO/IEC 27001:n, EU:n GDPR:n, EU:n NIS2-direktiivin ja EU:n DORA-asetuksen kanssa

9.1.2 Huomioida päivitetyt uhkat tai muutokset turvallisen kehityksen parhaissa käytännöissä

9.1.3 Varmistaa yhteensopivuus uusien työkalujen, alustojen tai toimittajasuhteiden kanssa

9.2 Välikatselmoinnit on käynnistettävä seuraavissa tilanteissa:

9.2.1 Ilmoitettu ohjelmistoon liittyvä tietoturvapoikkeama

9.2.2 Uuden kehitysviitekehyksen tai hosting-alustan käyttöönotto

9.2.3 Muutos kolmannen osapuolen kehityskumppaneissa

9.2.4 Ohjelmistoihin tai tietoturvavelvoitteisiin vaikuttavat sääntelymuutokset

9.3 Kaikki tähän politiikkaan tehtävät muutokset on:

9.3.1 Dokumentoitava päivämäärän, muutoksen yhteenvedon ja toimitusjohtajan (GM) hyväksynnän kanssa

9.3.2 Viestittävä selkeästi kaikelle sisäiselle ja ulkoiselle kehityshenkilöstölle

9.3.3 Säilytettävä osana organisaation politiikkojen versionhallintaa ja muutoshistoriaa

9.4 Päivitettyjen versioiden on oltava helposti saatavilla esimerkiksi sisäisten alustojen, painetun dokumentaation tai toimittajien käytettävissä olevien pilvipalvelujen kautta.

10. Liittyvät politiikat ja yhteydet

10.1 Tämä politiikka tukee useiden muiden pk-yrityksille tarkoitettujen politiikkojen onnistunutta toteutusta ja on niistä riippuvainen:

10.1.1 P2S – Hallintoroolien ja vastuiden politiikka: Määrittää vastuut kehityksen tietoturvakontrollien osoittamiselle ja varmentamiselle projektien ja toimittajien välillä.

10.1.2 P4S – Pääsynhallintapolitiikka: Määrittää perustason säännöt kehitysympäristöjen ja kooditietovarastojen käyttöoikeuksien rajoittamiselle, mukaan lukien tehtävien eriyttäminen.

10.1.3 P8S – Tietoturvatietoisuus- ja koulutuspolitiikka: Varmistaa, että sisäiset kehittäjät ja sopimuskumppanit ymmärtävät turvallisen ohjelmoinnin käytännöt ja niihin liittyvät tietoturvavastuut.

10.1.4 P17S – Tietosuoja- ja yksityisyydensuojapolitiikka: Selventää, miten henkilötietoja on käsiteltävä kehityksen, testauksen ja lokituksen aikana, jotta EU:n GDPR:n vaatimukset täyttyvät.

10.1.5 P30S – Tietoturvapoikkeamien hallintapolitiikka: Määrittää, miten kehitykseen liittyvät tietoturvapoikkeamat, mukaan lukien koodiin liittyvät altistumiset, on ilmoitettava, arvioitava ja korjattava.

10.2 Nämä politiikat muodostavat yhdessä kokonaisuuden, joka varmistaa, että turvallinen kehitys on toteutettavissa ja todennettavissa myös pienessä tai vähäisen teknisen kyvykkyyden organisaatiossa.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Kohta 8.1 – Edellyttää operatiivisten kontrollien, mukaan lukien turvallinen kehitys, toteutusta siten, että ne ovat linjassa liiketoimintatavoitteiden ja riskitason kanssa.

11.2 ISO/IEC 27002

11.2.1 Kontrolli 8.25 – Suosittelee tietoturvan integroimista koko ohjelmiston elinkaareen, mukaan lukien lähdekoodin hallinta, versionhallinta ja kehittäjien käyttöoikeudet.

11.2.2 Kontrolli 8.26 – Määrittää menetelmät sovellusten testaukselle ja tietoturvatoiminnallisuuksien varmentamiselle ennen tuotantokäyttöä.

11.2.3 Kontrolli 8.27 – Edellyttää, että kolmannen osapuolen kehittäjät noudattavat samoja kehitysstandardeja ja että heidän tietoturvavastuunsa on määritelty selkeästi.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3–SA-15 – Määrittävät turvalliset kehitysprosessit, mukaan lukien kehittäjien pääsynhallinta, testaus, uhkamallinnus ja dokumentointi.

11.3.2 SI-10 – Edellyttää, että kehittäjät tunnistavat ja lieventävät yleisiä ohjelmistojen heikkouksia sekä käyttävät automatisoituja työkaluja soveltuvin osin.

11.4 EU:n GDPR (2016/679)

11.4.1 Artikla 25 – "Sisäänrakennettu ja oletusarvoinen tietosuoja" velvoittaa integroimaan tietoturvan ja tietosuojan ohjelmistojen suunnitteluun ja kehitykseen erityisesti silloin, kun käsitellään henkilötietoja.

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

11.5.1 Artikla 21(2)(a), (e) ja (h) – Edellyttää turvallisen kehityksen politiikkoja, avoimen lähdekoodin käytön valvontaa sekä sovelluksiin liittyvän riskien lieventämisen dokumentointia keskeisissä ja tärkeissä toimijoissa.

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

11.6.1 Artiklat 6(7), 9(1)(c) ja 10(2)(c) – Asettavat kehityksen elinkaaren tietoturvavelvoitteita rahoitussektorin toimijoille, mukaan lukien pk-yritykset, erityisesti kriittisten ICT-järjestelmien osalta.

11.7 COBIT 2019

11.7.1 BAI03 – "Ratkaisujen tunnistamisen ja toteutuksen hallinta" tukee jäsenneltyjen kehityskontrollien toteutusta painottaen tietoturvaa, jäljitettävyyttä ja häiriönsietokykyä pk-yritysten rajoitteet huomioon ottaen.