					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P28					Asiakirjan nimi: **Ulkoistetun 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 8.1	Ei sovelleta
ISO/IEC 27002:2022	Kontrollit 5.19-5.22, 8	Ei sovelleta
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-10	Ei sovelleta
EU:n GDPR	Artiklat 28, 32	Ei sovelleta
EU:n NIS2-direktiivi	Artiklat 21(2)(a), (h), 23	Ei sovelleta
EU:n DORA-asetus	Artiklat 28(1), (2)	Ei sovelleta
COBIT 2019	APO10, BAI03, DSS	Ei sovelleta

1. Tarkoitus

1.1 Tämä politiikka määrittää pakolliset hallintakeinot ohjelmisto- ja järjestelmäkehityksen ulkoistamiselle ulkoisille toimittajille, sopimuskumppaneille tai kehitystoimistoille siten, että turvalliset käytännöt sisällytetään koko kehityksen elinkaareen.

1.2 Tämän politiikan tavoitteena on ehkäistä ulkoistetuista kehitystoimeksiannoista aiheutuvia tietoturvahaavoittuvuuksia, tiedon menetystä, immateriaalioikeuksien altistumista ja vaatimustenmukaisuuspoikkeamia.

1.3 Tämä politiikka asettaa vaatimukset toimittajahallinnalle, turvallisen ohjelmistokehityksen standardeille, käyttöoikeuksien hallinnalle, seuranta- ja valvontavelvoitteille sekä toimeksiannon päättämiseen liittyville menettelyille, jotta kehitetyn ohjelmiston luottamuksellisuus, eheys ja saatavuus turvataan.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia organisaation yksiköitä, jotka käyttävät ulkoisia tahoja ohjelmisto- tai järjestelmäkehityksessä, mukaan lukien:

2.1.1 verkkosovellukset, mobiilisovellukset, sulautetut järjestelmät, ohjelmointirajapinnat, skriptit, automaatiotyönkulut tai alustamoduulit

2.1.2 räätälöity kehitys sisäisille alustoille, asiakasrajapinnan järjestelmille tai kaupallisille tuotteille

2.1.3 toimeksiannot kolmannen osapuolen kehittäjien, freelancereiden, toimistojen tai offshore-tiimien kanssa

2.2 Tämä politiikka koskee myös kaikkia ulkoisia tahoja, joilla on kehityksen aikana pääsy lähdekoodiin, testausympäristöihin tai CI/CD-putkiin.

2.3 Vaatimukset ovat sitovia riippumatta sopimustyypistä, kehitysmenetelmästä tai ulkoistetun palveluntarjoajan maantieteellisestä sijainnista.

3. Tavoitteet

3.1 Varmistaa turvallisen järjestelmäkehityksen elinkaaren käytäntöjen soveltaminen kaikissa ulkoistetuissa toimeksiannoissa suunnittelusta käyttöönoton jälkeiseen validointiin.

3.2 Varmistaa, että kaikki ulkoisten kehittäjien kanssa tehtävät sopimukset sisältävät pakolliset ehdot tietosuojasta, turvallisesta ohjelmistokehityksestä ja immateriaalioikeuksien säilymisestä organisaatiolla.

3.3 Määrittää pääsynhallinnan, seurannan ja auditoinnin vaatimukset kolmannen osapuolen kehittäjille, jotka käyttävät sisäisiä järjestelmiä.

3.4 Suojata organisaatiota toimitusketjun vaarantumiselta, oikeudellisilta rikkomuksilta ja ulkoisesti kehitettyihin ohjelmistoihin liittyvältä mainehaitalta.

3.5 Ylläpitää jatkuvaa vaatimustenmukaisuutta tietoturvaviitekehysten kanssa, mukaan lukien ISO/IEC 27001, NIST, EU:n GDPR, EU:n NIS2-direktiivi, EU:n DORA-asetus ja COBIT 2019.

4. Roolit ja vastuut

4.1 Ylin johto

4.1.1 Hyväksyy korkean riskin ulkoistetut kehityshankkeet ja hyväksyy politiikasta tehdyt perustellut poikkeukset.

4.1.2 Varmistaa, että ulkoistamispäätökset ovat linjassa strategisten tavoitteiden ja organisaation riskinottohalukkuuden kanssa.

4.2 Tietoturvajohtaja (CISO)

4.2.1 Hyväksyy toimittajan käyttöönoton tietoturvan näkökulmasta.

4.2.2 Määrittää ulkoistettuja toimeksiantoja koskevat tietoturvan hallintakeinovaatimukset ja katselmoi poikkeamaraportit.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Tämä politiikka on katselmoitava vähintään kerran vuodessa tai useammin seuraavissa tilanteissa:

9.1.1 uusien kehityksen ulkoistamismallien, toimittajien tai lainkäyttöalueiden käyttöönotto

9.1.2 muutokset sääntelyviitekehyksiin, kuten EU:n GDPR:ään, EU:n NIS2-direktiiviin tai EU:n DORA-asetukseen

9.1.3 ulkoistettuun koodiin, käyttöoikeuksiin tai toimituksiin liittyvän tietoturvapoikkeaman jälkeen

9.1.4 osana sisäisen tarkastuksen auditointihavaintoja tai tietoturvallisuuden hallintajärjestelmän parannuksia

9.2 Tietoturvajohtaja (CISO) vastaa politiikan katselmoinnin käynnistämisestä ja koordinoinnista kuullen seuraavia tahoja:

9.2.1.1 laki- ja hankintatoiminto (sopimusvelvoitteiden soveltamisen yhdenmukaisuuden varmistamiseksi)

9.2.1.2 projekti- ja tuoteomistajat (toiminnallisen toteuttamiskelpoisuuden varmistamiseksi)

9.2.1.3 tietoturvatoiminto (uhka- ja hallintakeinopäivityksiä varten)

9.2.1.4 ylin johto (lopullista hyväksyntää varten)

9.3 Kaikkien politiikkapäivitysten on oltava:

9.3.1.1 versiohallittuja ja tallennettuja nimettyyn dokumenttirekisteriin

9.3.1.2 viestittyjä sidosryhmille, jotka osallistuvat ulkoistettuun kehitystoimintaan

9.3.1.3 yhdistettyjä kaikkiin liittyvien politiikkojen tai menettelydokumentaation päivityksiin

9.4 Jokaiseen politiikkaversioon on liitettävä muutosloki, jotta muutosten ja hyväksyntöjen jäljitettävyys varmistetaan.

10. Liittyvät politiikat ja yhteydet

10.1 Tämä politiikka tukee seuraavia asiakirjoja ja saa niistä tukea:

10.1.1 P1 - Tietoturvapolitiikka: määrittää organisaatiotason tietoturvaperiaatteet, joita sovelletaan sekä sisäisessä kehityksessä että kolmansien osapuolten kehityksessä.

10.1.2 P5 - Muutoksenhallintapolitiikka: varmistaa, että kaikki ulkoistetuista koodipohjista aiheutuvat käyttöönottoon liittyvät muutokset katselmoidaan ja hyväksytään ennen toteutusta.

10.1.3 P13 - Tiedon luokittelu- ja merkintäpolitiikka: määrittää, miten arkaluonteiset tiedot tunnistetaan ennen niiden altistamista kehitystoimittajille tai tietovarastoille.

10.1.4 P18 - Kryptografisten hallintakeinojen politiikka: ohjaa, miten avaimia, salaisuuksia ja arkaluonteisia tunnistetietoja on käsiteltävä kehityksen ja toimituksen aikana.

10.1.5 P24 - Turvallisen kehittämisen politiikka: määrittää sisäisen ja ulkoisen ohjelmistokehityksen perusvaatimukset.

10.1.6 P30 - Tietoturvapoikkeamien hallintapolitiikka: ohjaa, miten ulkoistettuun kehitykseen liittyvät tietoturvaloukkaukset tai tietoturvaongelmat eskaloidaan, tutkitaan ja ratkaistaan.

10.1.7 P33 - Auditointi- ja vaatimustenmukaisuuden seurantapolitiikka: määrittää vaatimukset ulkoistetun kehitystoiminnan katselmoinnille auditointien tai vaatimustenmukaisuuskatselmusten aikana.

11. Viitestandardit ja viitekehykset

11.1 Tämä politiikka on yhdenmukaistettu kansainvälisesti tunnustettujen tietoturvaviitekehysten ja säädösten kanssa, jotta ohjelmistokehityksen turvallinen ulkoistaminen ja toimittajahallinnan käytännöt varmistetaan.

11.2 ISO/IEC 27001

11.2.1 Kohta 8.1 - toiminnan suunnittelu ja ohjaus: edellyttää prosessikontrolleja turvalliselle kehittämiselle ja kolmannen osapuolen toimituksille.

11.3 ISO/IEC 27002:2022 - kontrollit 5.19-5.21, 8

11.3.1 Liite A, kontrolli 5.19 - toimittajasuhteiden hallinta: edellyttää muodollisia sopimuksia, jotka sisältävät tietoturva- ja vaatimustenmukaisuusehtoja.

11.3.2 Liite A, kontrolli 5.20 - tietoturvan käsittely toimittajasopimuksissa: varmistaa, että kehitystä koskevat hallintakeinot sisällytetään sopimuksiin.

11.3.3 Liite A, kontrolli 5.21 - toimittajapalvelujen toimituksen hallinta: kattaa kolmannen osapuolen kehitystoimitusten ja riskien seurannan.

11.3.4 Liite A, kontrolli 8.27 - ulkoistettu kehittäminen: edellyttää määriteltyjä tietoturvavaatimuksia ja pääsynhallintaa ulkoisesti kehitetylle ohjelmistolle.

11.3.5 Nämä kontrollit määrittävät rakenteiset vaatimukset ulkoistettujen kehittäjien valinnalle, sopimiselle ja valvonnalle, mukaan lukien turvallisen kehittämisen käytännöt, koodin käsittely ja suorituskyvyn validointi.

11.4 NIST SP 800-53 Rev.5

11.4.1 SA-4 - hankintaprosessi: edellyttää, että turvallisen kehittämisen vaatimukset määritellään hankinnan yhteydessä.

11.4.2 SA-9 - ulkoiset järjestelmäpalvelut: ohjaa, miten kolmannen osapuolen kehittäjät käyttävät sisäisiä palveluita turvallisesti.

11.4.3 SA-10 - kehittäjän konfiguraationhallinta: vastaa ulkoisille tiimeille asetettuja versionhallinnan, koodin käyttöoikeuksien ja muutosten seurannan velvoitteita.

11.5 EU:n GDPR (2016/679)

11.5.1 Artikla 28 - käsittelijän velvollisuudet: edellyttää, että kolmannen osapuolen kehittäjien kanssa tehtävissä sopimuksissa määritellään henkilötietojen käsittelyä koskevat tietoturva-, hallintakeino- ja auditointivaatimukset.

11.5.2 Artikla 32 - käsittelyn turvallisuus: edellyttää asianmukaisia suojatoimia (esim. salaus, pääsynhallinta) kehitettäessä järjestelmiä, jotka käsittelevät henkilötietoja.

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

11.6.1 Artiklat 21(2)(a), (h), 23: edellyttävät, että turvallisen kehittämisen käytäntöjä sovelletaan kolmansien osapuolten toimeksiannoissa ja digitaalisissa toimitusketjuissa sekä että niihin kohdistuu valvontaa ja teknistä varmistusta.

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

11.7.1 Artiklat 28(1), (2): edellyttävät, että finanssialan toimijat hallitsevat ICT-kolmannen osapuolen riskejä sopimukseen perustuvilla hallintakeinoilla ja turvallisen kehittämisen valvonnalla erityisesti kriittisessä ulkoistetussa kehityksessä.

11.8 COBIT 2019

11.8.1 APO10 - toimittajien hallinta: määrittää rakenteiset vaatimukset toimittajien arvioinnille, sopimuksille ja suorituskyvyn seurannalle.

11.8.2 BAI03 - ratkaisujen rakentamisen hallinta: kohdistuu suoraan turvallisen järjestelmäkehityksen elinkaaren prosesseihin, koodikatselmointeihin ja kehityksen validointiin.

11.8.3 DSS05 - tietoturvapalvelujen hallinta: vastaa ulkoisesti tai kolmansien osapuolten kehittämien järjestelmien valvonnasta ja suojaamisesta.