					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P28S					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/säädös	Kohta/artikla	Kommentti
ISO/IEC 27001:2022	Kohdat 5.1, 6.1, 8	Sovellettavat tietoturvallisuuden hallintajärjestelmää ja toimittajia koskevat kontrollit
ISO/IEC 27002:2022	Kontrollit 5.19, 5.20, 8.25–8.27	Toimittajia ja turvallisen kehittämisen elinkaarta koskevat kontrollit
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-11, SA-15, SR-3	Hankintaa, toimitusketjua, turvallista kehittämistä ja toimittajasopimuksia koskevat vaatimukset
EU:n GDPR	Artikla 28	Kolmannen osapuolen suorittamaa käsittelyä koskevat sopimus- ja tietosuojavaatimukset
EU:n NIS2-direktiivi	Artikla 21(2)(a), (h)	Toimitusketjua ja turvallista sovelluskehitystä koskevat kontrollit
EU:n DORA-asetus	Artikla 10	ICT-kolmannen osapuolen riskien hallinta, mukaan lukien ulkoistettu kehitys
COBIT 2019	BAI03, DSS05	Ulkoistettua kehitystä ja ulkoisia IT-palveluntarjoajia koskevat vaatimukset

1. Tarkoitus

1.1 Tämän politiikan tarkoituksena on varmistaa, että kaikki ulkoistettu ohjelmistokehitys – riippumatta siitä, toteuttavatko sen freelancerit, toimistot tai kolmannen osapuolen palveluntarjoajat – toteutetaan turvallisesti, sopimuksellisesti hallitusti sekä sovellettavien lakisääteisten, sääntelyyn liittyvien ja auditointivaatimusten mukaisesti.

1.2 Politiikan tarkoituksena on suojata organisaatiota turvattomaan koodiin, epäselvään omistajuuteen, tietojen altistumiseen ja toimittajien puutteelliseen hallintaan liittyviltä riskeiltä edellyttämällä velvoittavia kehitysstandardeja ja toimittajavalvontaa myös silloin, kun organisaatiolla ei ole erillistä IT-osastoa.

1.3 Tämä politiikka tukee ISO/IEC 27001:2022 -sertifiointia määrittämällä selkeät kehitystä koskevat vaatimukset, vastuut ja dokumentoidut kontrollit kolmannen osapuolen kehitystoiminnalle.

2. Soveltamisala

2.1 Tämä politiikka koskee:

2.1.1 kaikkia ulkoistettuja kehittäjiä, mukaan lukien freelancerit ja kehitystoimistot

2.1.2 kaikkea kehitystyötä, joka liittyy sisäisiin työkaluihin, julkisille rajapinnoille altistuviin verkkosivustoihin, ohjelmistosovelluksiin tai liiketoiminnan automaatioon

2.1.3 henkilöstöä, joka vastaa ulkoisten kehittäjien valinnasta, hallinnasta tai valvonnasta

2.1.4 kaikkea kolmannen osapuolen järjestelmäintegraatiota, skriptausta tai kehitystä, joka on vuorovaikutuksessa yrityksen tietojen tai järjestelmien kanssa

2.2 Politiikka koskee myös kaikkia osapuolia ja alustoja, joilla on pääsy yrityksen tunnistetietoihin, tietovarastoihin, lähdekoodivarastoihin, testiympäristöihin tai tuotantojärjestelmiin.

3. Tavoitteet

3.1 Varmistaa, että kaikki ulkoistettu kehitys noudattaa turvallisen ohjelmoinnin periaatteita ja että kehittäjät ovat sopimuksellisesti velvoitettuja noudattamaan dokumentoituja standardeja ja salassapitovelvoitteita.

3.2 Määrittää omistajuus kaikille tuotoksille – koodille, omaisuuserille, tunnistetiedoille ja dokumentaatiolle – siten, että oikeudet siirtyvät kokonaisuudessaan yritykselle ja että luovutus projektin päättyessä on jäljitettävissä.

3.3 Ehkäistä yleisiä kehitykseen liittyviä riskejä, kuten suojatun koodin luvatonta uudelleenkäyttöä, kirjastojen kautta toteutuvia toimitusketjuhyökkäyksiä, tuettomien viitekehysten käyttöä ja arvioimattomia ylläpitäjäoikeuksia.

3.4 Edellyttää ennen toimeksiannon aloittamista dokumentaatiota jokaiselle ulkoistetulle projektille, mukaan lukien sopimukset, salassapitosopimus (NDA) ja vähimmäistietoturvavaatimukset.

3.5 Suojata asiakastietoja, järjestelmiä ja sisäisiä prosesseja edellyttämällä tehokasta kehityksen valvontaa, toimituksen jälkeistä testausta ja järjestelmien käyttöoikeuksien turvallista hallintaa.

4. Roolit ja vastuut

4.1 Toimitusjohtaja

4.1.1 hyväksyy kaikki toimittajasuhteet ja allekirjoittaa kehityssopimukset

4.1.2 varmistaa, että kaikki ulkoistettu kehitys noudattaa tätä politiikkaa

4.1.3 poistaa pääsyn yrityksen järjestelmiin projektin päätyttyä

4.1.4 katselmoi toimituksen jälkeisen dokumentaation ja tulokset

4.2 Projektin omistaja (tyypillisesti sisäinen työntekijä tai nimetty koordinaattori)

4.2.1 vastaa päivittäisestä koordinoinnista ulkoisen kehittäjän kanssa

4.2.2 varmistaa, että toiminnalliset vaatimukset täyttyvät ja tuotokset testataan

4.2.3 varmistaa koodin ja tunnistetietojen turvallisen luovutuksen

4.2.4 raportoi toimitusjohtajalle kaikki kehitykseen liittyvät ongelmat tai tietoturvapoikkeamat

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Vuosittainen katselmointi

9.1.1 Toimitusjohtajan on katselmoitava tämä politiikka vähintään kerran vuodessa. Katselmoinnilla varmistetaan, että politiikka täyttää edelleen:

9.1.1.1 ISO/IEC 27001 -sertifioinnin vaatimukset

9.1.1.2 lakisääteisten velvoitteiden muutokset (esim. EU:n GDPR:n artikla 28, DORA-asetuksen artikla 10)

9.1.1.3 pk-yritystason nykyiset kehityskäytännöt ja kolmannen osapuolen riskit

9.2 Väliaikaiset katselmoinnit

9.2.1 Politiikka on katselmoitava myös, kun:

9.2.1.1 uusi ulkoistetun kehityksen toimittaja tai alusta otetaan käyttöön

9.2.1.2 tapahtuu merkittävä ulkoistettuun kehitykseen liittyvä tietoturvapoikkeama

9.2.1.3 käytetyissä työkaluissa, alustoissa tai ympäristöissä tapahtuu olennaisia muutoksia

9.3 Katselmointiprosessi

9.3.1 Toimitusjohtaja vastaa siitä, että:

9.3.1.1 sopimusten, salassapitosopimusten (NDA) ja pääsynhallintaprosessien tehokkuus varmistetaan

9.3.1.2 vahvistetaan, että nykyiset toimittajat ja freelancerit noudattavat tätä politiikkaa

9.3.1.3 ehtoja päivitetään aiemmista projekteista tai tietoturvapoikkeamista saadun palautteen perusteella

9.4 Versionhallinta ja viestintä

9.4.1 Kaikki muutokset on:

9.4.1.1 kirjattava päivämäärän, syyn ja muutoksen kuvauksen kanssa

9.4.1.2 hyväksytettävä toimitusjohtajalla ja lisättävä versiohistoriaan

9.4.1.3 viestittävä kaikelle henkilöstölle tai projektin omistajille, jotka työskentelevät ulkoisten kehittäjien kanssa

9.4.1.4 jaettava uudelleen kaikille asiaankuuluville toimittajille ja kolmansille osapuolille tarvittaessa

10. Liittyvät politiikat ja yhteydet

10.1 Tämä politiikka tukee suoraan seuraavien pk-yrityksille sovitettujen politiikkojen toimeenpanoa ja on niistä riippuvainen:

10.1.1 P2S – Hallintoroolien ja vastuiden politiikka: selventää, kuka vastaa toimittajien hyväksynnästä, pääsynhallinnasta ja riskin hyväksynnästä ulkoistettuja kehittäjiä käytettäessä.

10.1.2 P4S – Pääsynhallintapolitiikka: määrittää käyttäjätilien ja ylläpitäjäoikeuksien asianmukaisen luomisen, rajoittamisen ja poistamisen ulkoistetun kehityksen aikana.

10.1.3 P8S – Tietoturvatietoisuus- ja koulutuspolitiikka: varmistaa, että sisäinen henkilöstö ymmärtää, miten ulkoisten kehittäjien kanssa toimitaan turvallisesti, mukaan lukien tunnistetietojen ja projektitiedostojen käsittely.

10.1.4 P17S – Tietosuoja- ja yksityisyydensuojapolitiikka: määrittää tietoturva- ja oikeudelliset vaatimukset sellaisten henkilötietojen käsittelylle, joita ulkoistetut kehittäjät voivat käsitellä EU:n GDPR:n mukaisesti.

10.1.5 P24S – Turvallisen kehittämisen politiikka: määrittää, miten sisäisen ja ulkoisen kehityksen on noudatettava turvallisen ohjelmoinnin käytäntöjä sekä kirjastojen ja viitekehysten arviointia.

10.1.6 P30S – Tietoturvapoikkeamien hallintapolitiikka: sitä sovelletaan, kun ulkoistettu kehitys johtaa tietoturvapoikkeamiin tai haavoittuvuuksiin, ja se ohjaa koordinoitua tutkintaa sekä korjaavia toimenpiteitä.

10.2 Nämä politiikat on toimeenpantava rinnakkain sen varmistamiseksi, ettei ulkoistettu kehitys aiheuta hallitsematonta riskiä tai johda pk-yrityksen vaatimustenmukaisuusvelvoitteiden rikkomiseen.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Kohta 6.1 – Organisaation on arvioitava ja käsiteltävä toimittajiin liittyvät tietoturvariskit.

11.1.2 Kohta 8.1 – Edellyttää operatiivista suunnittelua ja ohjausta, mukaan lukien kolmannen osapuolen palvelut, kuten ulkoistettu kehitys.

11.2 ISO/IEC 27002

11.2.1 Kontrolli 5.19 – Suosittelee arvioimaan toimittajien kykyä täyttää tietoturvavaatimukset.

11.2.2 Kontrolli 5.20 – Suosittelee kolmannen osapuolen palvelujen säännöllistä seurantaa ja määräajoin tehtävää katselmointia.

11.2.3 Kontrollit 8.25–8.27 – Kuvaavat turvallisen kehittämisen elinkaaren käytäntöjä, joita sovelletaan ulkoistettuun kehitykseen.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-4 – Edellyttää, että hankintastrategiat sisältävät tietoturvatoimenpiteet.

11.3.2 SA-9 – Käsittelee ulkoista järjestelmäkehitystä ja toimitusketjuriskejä.

11.3.3 SA-11 – Määrittää turvallisen kehittämisen käytännöt, mukaan lukien koodikatselmoinnit ja puutteiden korjaamisen.

11.3.4 SA-15 – Suosittelee automatisoituja työkaluja puutteiden havaitsemiseen ja ohjelmistovarmennukseen.

11.3.5 SR-3 – Edellyttää, että toimittajasopimukset sisältävät kyberturvallisuusvaatimukset.

11.4 Euroopan unionin yleinen tietosuoja-asetus (GDPR)

11.4.1 Artikla 28 – Edellyttää sopimuksia kolmannen osapuolen henkilötietojen käsittelijöiden kanssa asianmukaisten tietosuojatoimenpiteiden varmistamiseksi; tämä koskee suoraan kehittäjiä, jotka käsittelevät henkilötietoja tai joilla on niihin pääsy.

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

11.5.1 Artikla 21(2)(a), (h) – Edellyttää toimitusketjun tietoturvakontrolleja ja turvallisen ohjelmistokehityksen käytäntöjä soveltamisalaan kuuluvilta digitaalisilta palveluntarjoajilta, mukaan lukien pk-yritykset soveltuvin osin.

11.6 EU:n digitaalista häiriönsietokykyä koskeva asetus (DORA)

11.6.1 Artikla 10 – Edellyttää ICT-kolmannen osapuolen riskien hallintaa, mukaan lukien kehityssopimukset, tietoturvavelvoitteet ja kolmannen osapuolen palveluntarjoajiin liittyvät riskikontrollit.

11.7 COBIT 2019

11.7.1 BAI03 – Ratkaisujen tunnistamisen ja rakentamisen hallinta – varmistaa, että ulkoinen kehitys täyttää liiketoimintavaatimukset ja tietoturvaa koskevat odotukset.

11.7.2 DSS05 – Tietoturvapalvelujen hallinta – edellyttää, että ulkoiset tietoturvapalvelut ja kehityspalveluntarjoajat toimivat velvoittavien tietoturvasääntöjen ja valvonnan alaisina.