					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P25					Asiakirjan nimi: **Sovellustietoturvavaatimusten 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	Lauseke/artikla	Kommentti
ISO/IEC 27001:2022	Lauseke 8	—
ISO/IEC 27002:2022	Kontrollit 8.25–8.26	—
NIST SP 800-53 Rev.5	SA-11, SA-15, SI-10	—
EU:n GDPR	Artiklat 25, 32	—
EU:n NIS2-direktiivi	Artiklat 21(2)(f), 23	—
EU:n DORA-asetus	Artiklat 9, 11	—
COBIT 2019	BAI03, BAI09, DSS05	—

1. Tarkoitus

1.1 Tämä politiikka määrittää pakolliset sovellustason tietoturvavaatimukset organisaation kehittämille, hankkimille, integroiduille tai käyttöön otetuille ohjelmistoille. Se varmistaa, että kaikki sovellukset suunnitellaan, toteutetaan ja ylläpidetään turvallisen kehittämisen periaatteiden, sääntelyvaatimusten ja organisaation riskinottohalukkuuden mukaisesti.

1.2 Tämä politiikka edellyttää tietoturvan sisällyttämistä koko sovelluksen elinkaareen kattaen käyttäjien todentamisen, tietojen käsittelyn, rajapintojen suojaamisen sekä turvallisen vuorovaikutuksen ohjelmointirajapintojen ja palveluiden kanssa.

1.3 Tämän politiikan tarkoituksena on ehkäistä ohjelmistohaavoittuvuuksien syntymistä, suojata arkaluonteisia tietoja sekä varmistaa jäljitettävyys ja häiriönsietokyky hyväksikäyttöyrityksiä ja väärinkäyttöä vastaan.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia seuraavia:

2.1.1 organisaation sisäisesti kehitettyjä tai ulkoisesti hankittuja sovelluksia, mukaan lukien SaaS-palvelut ja räätälöidyt työkalut

2.1.2 sovelluksia, jotka tukevat kriittisiä liiketoimintatoimintoja, asiakaskäyttöä tai sääntelyn alaisten tietojen käsittelyä

2.1.3 kehitys-, DevOps-, laadunvarmistus-, tuote- ja tietoturvatiimejä

2.1.4 kolmannen osapuolen kehittäjiä, ohjelmistotoimittajia ja integraatiokumppaneita, joilla on pääsy organisaation sovelluksiin tai ohjelmointirajapintoihin

2.2 Tätä politiikkaa sovelletaan kaikkiin ympäristöihin: kehitys-, testaus-, staging-, tuotanto- ja katastrofipalautusympäristöihin riippumatta siitä, sijaitsevatko ne organisaation omissa tiloissa, yksityisissä konesaleissa vai julkisissa pilviympäristöissä.

3. Tavoitteet

3.1 Määrittää perustason toiminnalliset ja ei-toiminnalliset tietoturvavaatimukset, jotka kaikkien sovellusten on täytettävä riippumatta kehitysmenetelmästä tai teknologiakokonaisuudesta.

3.2 Varmistaa sovellustason suojausmekanismien integrointi, mukaan lukien syötteiden validointi, tulosteiden koodaus, virheenkäsittely ja istuntojen suojaus.

3.3 Edellyttää todentamis-, valtuutus- ja pääsynhallintamekanismien turvallista toteutusta organisaation identiteetin- ja pääsynhallintapolitiikkojen mukaisesti.

3.4 Velvoittaa toteuttamaan turvallisen vuorovaikutuksen ohjelmointirajapintojen, verkkorajapintojen ja kolmannen osapuolen komponenttien kanssa käyttäen hyväksyttyjä protokollia ja tietoturvakontrolleja.

3.5 Mahdollistaa haavoittuvuuksien varhaisen havaitsemisen ja lieventämisen staattisen ja dynaamisen analyysin, koodikatselmointien ja uhkamallinnuksen avulla.

3.6 Suojata arkaluonteiset tiedot sääntelyvaatimusten mukaisesti toteuttamalla salaus, luokittelu ja tietojen säilytyslogiikka.

3.7 Varmistaa sovellusten tietoturvatilan jatkuva validointi käyttöönoton jälkeen testauksen, seurannan ja auditointivalmiuden avulla.

4. Roolit ja vastuut

4.1 Tietoturvajohtaja (CISO)

4.1.1 Omistaa tämän politiikan ja varmistaa sen yhdenmukaisuuden organisaation tietoturvastrategian ja riskitason kanssa.

4.1.2 Hyväksyy sovellusturvallisuusvaatimukset ja varmistaa pakollisten kontrollien toteutuksen kehitys- ja hankintatoiminnoissa.

4.2 Sovellusturvallisuudesta vastaava henkilö / DevSecOps-päällikkö

4.2.1 Määrittää sovelluskomponenttien perustason tietoturvakontrollit ja testausmenetelmät.

4.2.2 Valvoo työkalujen, kuten SAST:n, DAST:n, IAST:n ja SCA:n, turvallista integrointia ohjelmistotoimitusputkeen.

4.2.3 Ylläpitää sovellusturvallisuusvaatimusten tarkistuslistaa ja validointikriteerejä.

[... 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 seuraavissa tilanteissa:

9.1.1 kriittiset haavoittuvuusilmoitukset, jotka vaikuttavat yleisesti käytettyihin viitekehyksiin tai riippuvuuksiin

9.1.2 sovellusturvallisuuteen liittyvien sääntelyvaatimusten päivitykset, kuten EU:n NIS2-direktiivi tai DORA-asetus

9.1.3 merkittävät muutokset organisaation ohjelmistokehityskäytännöissä, työkalustossa tai pilviarkkitehtuurissa

9.1.4 sisäisen tarkastuksen tai ulkoisten penetraatiotestien havainnot

9.2 Katselmoinnista vastaa sovellusturvallisuudesta vastaava henkilö yhteistyössä tietoturvajohtajan (CISO), DevOps-kehityksen, laki- ja vaatimustenmukaisuustoiminnon, hankinnan ja laadunvarmistuksesta vastaavien kanssa.

9.3 Kaikkien muutosten on oltava versiohallittuja ISMS:n asiakirjahallintarekisterissä, ja ne on jaettava kaikille asiaankuuluville kehitys- ja tuotetiimeille.

9.4 Korvatut versiot on arkistoitava vähintään kolmeksi vuodeksi jäljitettävyyden, todennettavuuden ja tietomurtotutkinnan tueksi.

10. Liittyvät politiikat ja yhteydet

10.1 P1 – Tietoturvapolitiikka. Määrittää järjestelmien ja tietojen suojaamisen perustan, jonka pohjalta sovellustason kontrollit on toteutettava luvattoman pääsyn, tietovuotojen ja hyväksikäyttöyritysten estämiseksi.

10.2 P4 – Pääsynhallintapolitiikka. Määrittää identiteetin- ja istunnonhallinnan standardit, jotka kaikkien sovellusten on toteutettava, mukaan lukien vahva tunnistautuminen, vähimmän oikeuden periaate ja käyttöoikeuksien katselmointivaatimukset.

10.3 P5 – Muutoksenhallintapolitiikka. Sääntelee sovelluskoodin ja konfiguraatioiden siirtämistä tuotantoympäristöihin varmistaen, että luvattomat tai testaamattomat muutokset estetään.

10.4 P17 – Tietosuoja- ja yksityisyydensuojapolitiikka. Edellyttää, että sovelluksissa toteutetaan sisäänrakennettu tietosuoja sekä varmistetaan henkilötietojen ja arkaluonteisten tietojen lainmukainen käsittely, salaus ja säilytys kaikissa ympäristöissä.

10.5 P24 – Turvallisen kehittämisen politiikka. Tarjoaa laajemman viitekehyksen tietoturvan sisällyttämiseksi järjestelmäkehityksen elinkaareen, ja tämä politiikka määrittää sovellustasolla toteutettavat konkreettiset vaatimukset ja tekniset kontrollit.

10.6 P30 – Tietoturvapoikkeamien hallintapolitiikka. Velvoittaa käsittelemään sovellusturvallisuuteen liittyvät tietoturvapoikkeamat jäsennellysti, mukaan lukien käyttöönoton jälkeen tai penetraatiotestauksen aikana tunnistetut haavoittuvuudet, ja määrittää eskalointi-, rajaamis- ja palautumismenettelyt.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001:2022

11.1.1 Lauseke 8.1 – Toiminnan suunnittelu ja ohjaus: Edellyttää, että sovellusturvallisuus sisällytetään prosesseihin ja järjestelmiin luottamuksellisuuden, eheyden ja saatavuuden varmistamiseksi.

11.2 ISO/IEC 27002:2022

11.2.1 Kontrollit 8.25–8.26: Määrittävät sovellustason tietoturvaa koskevat odotukset, mukaan lukien turvallisen ohjelmoinnin käytännöt, uhkamallinnus, arkkitehtuurikontrollit ja kolmannen osapuolen ohjelmistojen validointi.

11.2.2 Liite A, kontrolli 8.25 – Turvallinen kehityksen elinkaari: Velvoittaa integroimaan tietoturvan koko sovelluksen elinkaareen.

11.2.3 Liite A, kontrolli 8.26 – Sovellusturvallisuusvaatimukset: Velvoittaa määrittämään ja toteuttamaan tekniset kontrollit sovellusten suojaamiseksi väärinkäytöltä ja vaarantumiselta.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Kehittäjän tietoturvatestaus ja arviointi: Edellyttää staattista ja dynaamista testausta sekä penetraatiotestausta kehityksen aikana.

11.3.2 SA-15 – Kehitysprosessi, standardit ja työkalut: Määrittää muodolliset standardit turvalliselle sovelluskehitykselle.

11.3.3 SI-10 – Tietosyötteen validointi: Edellyttää kontrollimekanismeja injektio- ja jäsennyshyökkäysten estämiseksi.

11.4 EU:n GDPR (2016/679)

11.4.1 Artikla 25 – Sisäänrakennettu ja oletusarvoinen tietosuoja: Edellyttää tietosuojan ja yksityisyydensuojan sisällyttämistä sovelluslogiikkaan ja työnkulkuihin.

11.4.2 Artikla 32 – Käsittelyn turvallisuus: Velvoittaa asianmukaisiin teknisiin toimenpiteisiin, kuten syötteiden validointiin, salaukseen ja turvallisiin pääsynhallintakontrolleihin.

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

11.5.1 Artikla 21(2)(f): Edellyttää haavoittuvuuksien käsittelyä ja turvallisen sovelluksen elinkaaren käytäntöjä keskeisiltä ja tärkeiltä toimijoilta.

11.5.2 Artikla 23 – Tietoturvapoikkeamien ilmoittaminen: Edellyttää sovellustason lokitus- ja valvontakyvykkyyksiä merkittävien tietoturvapoikkeamien havaitsemiseksi ja ilmoittamiseksi.

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

11.6.1 Artikla 9 – ICT-riskien hallinta: Velvoittaa finanssialan toimijat varmistamaan, että sovellukset ovat turvallisia, testattuja ja kyberuhkia kestäviä.

11.6.2 Artikla 11 – ICT-työkalujen testaus: Kannustaa tekemään kriittisille sovelluksille ja palveluille säännöllistä penetraatiotestausta ja red team -harjoituksia.

11.7 COBIT 2019

11.7.1 BAI03 – Ratkaisujen tunnistamisen ja rakentamisen hallinta: Määrittää suunnittelu- ja kontrollivaatimukset sovelluskehityksen aikana.

11.7.2 BAI09 – Sovellusten hallinta: Korostaa käytössä olevien sovellusten turvallista ylläpitoa, seurantaa ja kehittämistä.

11.7.3 DSS05 – Tietoturvapalvelujen hallinta: Kytkee sovellusten suojauksen organisaation laajempiin tietoturvaoperaatioihin ja kontrollikokonaisuuksiin.