					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P25S					Asiakirjan nimi: **Sovellusten tietoturvavaatimusten politiikka - SME**							
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	Luku 8	Operatiiviset kontrollit, mukaan lukien sovellusturvallisuus
ISO/IEC 27002:2022	Kontrollit 8.25–8.26	Turvallinen suunnittelu, kehittäminen, testaus ja koodikatselmointi
NIST SP 800-53 Rev.5	SA-11, SI-10	Kehittäjän tai sovelluksen testaus, koodianalyysi ja virheiden ennaltaehkäisy
EU:n GDPR	Artikla 25	Sisäänrakennettu ja oletusarvoinen tietosuoja
EU:n NIS2-direktiivi	Artikla 21(2)(a), (e)	Tekniset toimenpiteet sovellusten suojaamiseksi ja riskien havaitsemiseksi
EU:n DORA-asetus	Artiklat 9(2)(c), 10(2)(c)	Sovellusturvallisuus digitaalisen toiminnan häiriönsietokyvyn varmistamiseksi
COBIT 2019	BAI03	Turvallisen ohjelmistokehityksen ja -hankinnan hallinta

1. Tarkoitus

1.1 Tämä politiikka määrittää pakollisten sovellusturvallisuuskontrollien vähimmäisvaatimukset, joita sovelletaan kaikkiin organisaation käyttämiin ohjelmistoihin ja järjestelmäratkaisuihin riippumatta siitä, kehitetäänkö ne sisäisesti vai hankitaanko ne ulkoisilta toimittajilta.

1.2 Tällä varmistetaan, että sovellukset suunnitellaan, toteutetaan ja ylläpidetään siten, että asiakkaiden, työntekijöiden ja liiketoimintatietojen suojaus luvattomalta pääsyltä, väärinkäytöltä, muuttamiselta ja tuhoamiselta toteutuu.

1.3 Tämä politiikka tukee organisaation tavoitteita saavuttaa ja ylläpitää ISO/IEC 27001 -sertifiointia, täyttää EU:n GDPR:n ja EU:n NIS2-direktiivin vaatimukset sekä vähentää tietoturvattomiin ohjelmistokäyttöönottoihin liittyviä operatiivisia riskejä.

1.4 Tämä politiikka auttaa luomaan pk-yrityksille yhdenmukaisen ja todennettavan lähestymistavan sovellusturvallisuuteen määrittämällä yhtenäisen tarkistuslistan tietoturvaominaisuuksista ja -käytännöistä ympäristöihin, joissa sisäiset tekniset resurssit ovat rajalliset.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia sovelluksia, järjestelmiä, työkaluja ja alustoja, jotka:

2.1.1 kehitetään sisäisesti, räätälöidään tai skriptataan sisäiseen käyttöön

2.1.2 hankitaan kaupallisina ohjelmistoina, SaaS-ratkaisuina tai pilvipohjaisina järjestelminä

2.1.3 käsittelevät, tallentavat tai siirtävät henkilötietoja, liiketoiminnan tietoaineistoja tai arkaluonteisia operatiivisia tietoja

2.1.4 ovat työntekijöiden, toimeksisaajien, asiakkaiden tai kumppaneiden käytettävissä sisäverkkojen, internetin tai mobiilialustojen kautta

2.2 Politiikka koskee seuraavia tahoja:

2.2.1 kehittäjät (sisäiset tai sopimussuhteiset)

2.2.2 ohjelmistotoimittajat ja pilvipalveluntarjoajat

2.2.3 IT-tukihenkilöstö tai järjestelmänvalvojat, jotka vastaavat käyttöönotosta ja tuesta

2.2.4 sovellusomistajat ja liiketoiminnan käyttäjät, jotka osallistuvat järjestelmän hyväksyntään ja valvontaan

3. Tavoitteet

3.1 Varmistaa, että kaikissa organisaation käyttämissä sovelluksissa on sisäänrakennetut ja todennettavissa olevat tietoturvakontrollit, jotka pienentävät yleisistä ohjelmistohaavoittuvuuksista aiheutuvaa riskiä.

3.2 Suojata sovellusten käsittelemien tietojen luottamuksellisuus, eheys ja saatavuus riippumatta siitä, missä ne on isännöity.

3.3 Edellyttää sovellusturvallisuuden muodollista testausta, katselmointia ja validointia ennen uuden sovelluksen tai merkittävän päivityksen hyväksymistä tuotantokäyttöön.

3.4 Mahdollistaa käyttäjätunnusten, istuntotietojen ja käyttöoikeuksien yhdenmukainen ja turvallinen käsittely kaikissa liiketoiminnan kannalta kriittisissä järjestelmissä.

3.5 Edellyttää kaikissa sovelluksissa turvallista lokitusta, auditointikyvykkyyksiä ja valvontaominaisuuksia epäilyttävän toiminnan havaitsemisen ja siihen reagoinnin tukemiseksi.

3.6 Vähentää oikeudellisia ja vaatimustenmukaisuusriskejä varmistamalla, että sovellukset täyttävät sovellettavat sääntelyperusteiset tietoturvavaatimukset.

4. Roolit ja vastuut

4.1 toimitusjohtaja

4.1.1 Vastaa kokonaisuutena sovellusturvallisuudesta koko organisaatiossa.

4.1.2 Hyväksyy tämän politiikan ja varmistaa, että kaikki hankinnat ja kehityshankkeet noudattavat sitä.

4.1.3 Varmistaa, että toimittajia ja palveluntarjoajia sitovat sopimuksellisesti sovellusturvallisuutta koskevat vaatimukset.

4.1.4 Katselmoi ja hyväksyy riskipoikkeukset tilanteissa, joissa täyttä vaatimustenmukaisuutta ei voida saavuttaa liiketoiminnallisista rajoitteista johtuen.

4.2 sovellusomistaja (jos nimetty)

4.2.1 Tunnistaa sovelluskohtaiset tietoturvatarpeet järjestelmän valinnan tai hankkeen käynnistämisen yhteydessä.

4.2.2 Varmistaa, että keskeiset ominaisuudet, kuten kirjautumisen suojaus, salaus ja tapahtumalokit, sisältyvät ratkaisuun.

4.2.3 Osallistuu käyttöönottoa edeltäviin katselmointeihin ja varmistaa, että tietoturvakontrollit vastaavat liiketoiminnan tarpeita.

[... 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 kalenterivuodessa, jotta voidaan:

9.1.1 huomioida muutokset sääntelyvaatimuksissa (esim. EU:n GDPR, EU:n NIS2-direktiivi, DORA-asetus)

9.1.2 sisällyttää uudet tai kehittyvät uhat ja hyökkäystekniikat

9.1.3 päivittää sanamuotoja ja vaatimuksia vastaamaan alustoissa, toimittajissa tai kehitysmenetelmissä tapahtuneita muutoksia

9.2 Välikatselmointeja on tehtävä myös silloin, kun:

9.2.1 otetaan käyttöön uusia sovelluksia

9.2.2 olemassa oleviin sovelluksiin tehdään merkittäviä päivityksiä tai integraatioita

9.2.3 tapahtuu sovellukseen liittyvä poikkeama tai tietoturvaloukkaus

9.2.4 uusia riskejä tunnistetaan ulkoisista tiedotteista tai toimialan hälytyksistä

9.3 Kaikkien tähän politiikkaan tehtävien päivitysten on oltava:

9.3.1 toimitusjohtajan hyväksymiä

9.3.2 dokumentoituja yhdessä versiohistorian ja muutoksen perustelun kanssa

9.3.3 viestittyjä kaikille työntekijöille, kehittäjille ja toimittajille, jotka osallistuvat sovellusten hallintaan

9.3.4 turvallisesti säilytettyjä auditointi- ja vaatimustenmukaisuusviittauksia varten

10. Liittyvät politiikat ja riippuvuudet

10.1 Tätä politiikkaa tukevat suoraan seuraavat pk-yrityksille sovitetut tietoturvapolitiikat, ja se edistää myös niiden toimeenpanoa:

10.1.1 P2S – Hallintoroolien ja vastuiden politiikka: Määrittää vastuut sovellusten hyväksymisestä, politiikan toimeenpanosta ja toimittajahallinnasta.

10.1.2 P4S – Pääsynhallintapolitiikka: Varmistaa, että sovellusten käyttöoikeudet toteutetaan vähimmän oikeuden periaatteen ja istunnonhallinnan periaatteiden mukaisesti.

10.1.3 P8S – Tietoturvatietoisuus- ja koulutuspolitiikka: Varmistaa, että käyttäjät ja kehittäjät saavat koulutuksen sovelluksiin liittyvien uhkien tunnistamiseen ja ilmoittamiseen.

10.1.4 P17S – Tietosuoja- ja yksityisyydensuojapolitiikka: Määrittää tietosuojavaatimukset, jotka on toteutettava kaikissa henkilötietoja käsittelevissä sovelluksissa.

10.1.5 P14S – Tietojen säilytys- ja hävityspolitiikka: Määrittää, miten sovellusten tuottamat lokit, varmuuskopiot ja arkaluonteiset tiedot on säilytettävä, arkistoitava ja hävitettävä turvallisesti.

10.1.6 P30S – Tietoturvapoikkeamien hallintapolitiikka: Kuvaa vaiheet sovelluksiin liittyvien tietoturvatapahtumien tunnistamiseen, ilmoittamiseen ja rajaamiseen.

10.2 Yhdessä nämä politiikat varmistavat, että sovellusturvallisuus on täysin integroitu organisaation tietoturvallisuuden hallintajärjestelmään (ISMS) ja että auditointivalmius säilyy.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Luku 8.1 – Edellyttää, että organisaatiot ottavat käyttöön operatiiviset kontrollit tietoturvariskien hallitsemiseksi, mukaan lukien sovelluksiin ja ohjelmistojärjestelmiin liittyvät riskit.

11.2 ISO/IEC 27002

11.2.1 Kontrolli 8.25 – Ohjeistaa ottamaan käyttöön turvallisen suunnittelun, kehittämisen ja koodikatselmoinnin käytännöt kaikissa sovelluksissa, mukaan lukien toimittajien tarjoamat sovellukset.

11.2.2 Kontrolli 8.26 – Suosittelee sovellusturvallisuuskontrollien muodollista testausta erityisesti pääsynhallinnan, syötteen validoinnin ja istunnonhallinnan osa-alueilla.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Määrittää vaatimukset kehittäjien suorittamalle testaukselle, koodianalyysille ja dynaamiselle sovellusskannaukselle ennen käyttöönottoa.

11.3.2 SI-10 – Käsittelee yleisten ohjelmistovirheiden havaitsemista ja estämistä painottaen kehittäjien tietoisuutta ja teknisiä suojatoimia.

11.4 EU:n GDPR (2016/679)

11.4.1 Artikla 25 – ”Sisäänrakennettu ja oletusarvoinen tietosuoja” edellyttää tietosuojan ja tietoturvan sisällyttämistä henkilötietoja käsittelevien sovellusten ydinsuunnitteluun.

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

11.5.1 Artikla 21(2)(a) ja (e) – Edellyttää keskeisiltä ja tärkeiltä toimijoilta teknisten toimenpiteiden toteuttamista sovellusten suojaamiseksi ja ohjelmistoihin liittyvien riskien havaitsemiseksi.

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

11.6.1 Artiklat 9(2)(c), 10(2)(c) – Edellyttävät finanssialan pk-yrityksiltä sovellustason tietoturvakontrollien sisällyttämistä ratkaisuihin sekä säännöllisiä arviointeja digitaalisen toiminnan häiriönsietokyvyn ylläpitämiseksi.

11.7 COBIT 2019

11.7.1 BAI03 – ”Manage Solutions Identification and Build” ohjaa turvallista ohjelmistokehitystä tai -hankintaa riskien, vaatimustenmukaisuuden ja liiketoimintavaatimusten mukaisesti myös resurssirajoitteisissa pk-yritysympäristöissä.