					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P24					Dokumendi pealkiri: **Turvalise arenduse poliitika**							
Versioon: 1.0		Jõustumiskuupäev: 01.01.2025			Dokumendi omanik:							
X	Poliitika		Standard		Protseduur		Vorm		Register		Muu	

Muudatuste ajalugu				
Muudatuse number	**Muudatuse kuupäev**	**Muudatused**	**Läbi vaadanud**	**Protsessi omanik**

Kinnitused			
Nimi	**Ametikoht**	**Kuupäev**	**Allkiri**

1. Eesmärk

1.1 Käesolev poliitika sätestab organisatsiooni tarkvara ja süsteemide arendustegevusele kohustuslikud turbenõuded, sealhulgas organisatsioonisisestele projektidele, allhanke korras teostatavale arendusele ja kolmandate osapoolte koodi integreerimisele.

1.2 Eesmärk on tagada, et turvalisus on lõimitud kogu tarkvaraarenduse elutsüklisse (SDLC) ning et haavatavused tuvastatakse, maandatakse ja ennetatakse enne tootmiskeskkonda juurutamist.

1.3 Käesolev poliitika toetab standardi ISO/IEC 27001:2022 punkti 8.1 ja lisa A kontrollimeetmete 8.25–8.28 rakendamist, standardides turvalise arenduse juhtimise, koodi valideerimise tavad ja kolmandate osapoolte arenduse järelevalve.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub järgmisele:

2.1.1 Organisatsioonisiseselt või väliselt arendatud tarkvara, rakendused, skriptid, integratsioonid ja automatiseerimisvahendid

2.1.2 Arendusmeeskonnad, tooteomanikud, DevOpsi meeskonnad, kvaliteeditagamise spetsialistid, arhitektid, projektijuhid ja töövõtjad

2.1.3 SDLC keskkonnad, sealhulgas arendus-, test-, vahe- ja eeltootmiskeskkonnad

2.1.4 Siserakendustesse integreeritud avatud lähtekoodiga ja kolmandate osapoolte komponendid

2.1.5 Tarkvara, mis on juurutatud kohapealses taristus, privaatpilve-, hübriidpilve- või avaliku pilve keskkondades

2.2 Käesolev poliitika kehtib kõigile kasutajatele ja üksustele, kes osalevad organisatsiooni kontekstis süsteemide arendamises, testimises või juurutamises, sealhulgas hallatud teenuse osutajatele (MSP-d) ja platvormitarnijatele.

3. Eesmärgid

3.1 Lõimida turbekontrollid tarkvaraarenduse kõikidesse etappidesse alates kavandamisest kuni juurutamiseni, tagades ennetava ja pideva riskide vähendamise.

3.2 Ennetada ärakasutatavate haavatavuste lisandumist, näiteks sisendiründe id, ebaturvalist autentimist ja kokkupuudet kolmandate osapoolte teadaolevate nõrkustega.

3.3 Kehtestada ja rakendada turvalise programmeerimise tavad kooskõlas OWASP-i, SANS CWE ja raamistikupõhiste juhistega.

3.4 Tagada, et kogu kood läbib enne juurutamist vastastikuse hindamise, automatiseeritud analüüsi ja turbevalideerimise.

3.5 Hallata arendusega seotud riske, mis tulenevad allhanke korras teostatavatest tegevustest, kolmandate osapoolte koodi kaasamisest ja avatud lähtekoodiga tarkvara taaskasutusest.

3.6 Kaitsta arendus-, test- ja vahekeskkondi loata juurdepääsu eest ning vältida tootmisandmete kasutamist ilma heakskiidetud andmete maskeerimise või anonüümimiseta.

3.7 Edendada arendajate, tootejuhtide ja kvaliteeditagamise spetsialistide turbeteadlikkust rollipõhise koolituse ja uute ohtude kohta tehtavate regulaarsete teavituste kaudu.

4. Rollid ja vastutused

4.1 infoturbejuht

4.1.1 Vastutab käesoleva poliitika eest ja tagab, et turvalise arenduse nõudeid rakendatakse kogu organisatsioonis.

4.1.2 Kinnitab turvalise programmeerimise standardid ja kolmandate osapoolte arenduslepingud.

4.1.3 Valideerib riskikäsitluse otsused lahendamata või edasi lükatud haavatavuste korral.

4.2 rakendusturbe juht / DevSecOpsi juht

4.2.1 Koostab, haldab ja edendab turvalise programmeerimise juhiseid.

4.2.2 Lõimib staatilise ja dünaamilise turbetestimise CI/CD torustikesse.

4.2.3 Viib läbi koodi turbeülevaatusi ja määratleb kohustuslikud parandusmeetmed.

[... Jaotised 4.3–8 ei ole selles eelvaates. Täieliku sisu saamiseks ostke täisdokument. ...]

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Käesolev poliitika tuleb läbi vaadata vähemalt kord aastas või sagedamini järgmiste asjaolude ilmnemisel:

9.1.1 olulised muudatused arendusmetoodikates või DevOpsi tööriistades;

9.1.2 olulised turvaintsidendid, mille põhjus seisneb rakenduse haavatavustes;

9.1.3 muudatused turvalise tarkvaraga seotud regulatiivsetes nõuetes (nt GDPR, DORA);

9.1.4 uued valdkonna standardid või ohuteave (nt OWASP Top 10, SLSA, MITRE CWE).

9.2 Poliitika läbivaatamist juhib rakendusturbe juht koostöös infoturbejuhiga, tarkvaraarhitektide, kvaliteeditagamise juhtide ja õigusnõustajaga (kolmandate osapoolte koodiga seotud mõjude korral).

9.3 Kõik muudatused tuleb registreerida ISMS-i dokumendihalduse registris, hallata versioonihalduse kaudu ning edastada mõjutatud meeskondadele väljalaskemärkmete või kohustusliku koolituse kaudu.

9.4 Varasemad versioonid tuleb säilitada arhiivrepositooriumis õigusliku jälgitavuse ja auditijälje tagamiseks.

10. Seotud poliitikad ja seosed

10.1 P1 – Infoturbepoliitika. Määratleb strateegilise kohustuse lõimida turvalisus kõikidesse infosüsteemidesse, mille üks peamisi operatiivseid kontrollimeetmeid on turvaline arendus.

10.2 P4 – Juurdepääsukontrolli poliitika. Määratleb kontrollimeetmed arenduskeskkondadele, repositooriumidele, ehitustööriistadele ja CI/CD torustikele juurdepääsu piiramiseks.

10.3 P5 – Muudatuste haldamise poliitika. Tagab, et koodimuudatustele, väljalasetele ja juurutustele kohaldatakse nõuetekohast kinnitamist, tagasipööramise planeerimist ja juurutusjärgset kontrolli.

10.4 P12 – Varahalduse poliitika. Toetab arenduskeskkondade, lähtekoodi repositooriumide ja ehitussüsteemide käsitlemist hallatavate varadena, mille suhtes kehtivad klassifitseerimise ja kaitse nõuded.

10.5 P22 – Logimise ja seire poliitika. Kohaldub arendustorustikele, tagades, et ehitusprotsessid, koodi edutamised ja juurutussündmused logitakse, seiratakse ja analüüsitakse turbeanomaaliate tuvastamiseks.

10.6 P30 – Intsidentidele reageerimise poliitika (P30). Annab raamistiku juurutusjärgselt või rakendusturbe testimisel avastatud turvanõrkuste analüüsimiseks ja käsitlemiseks.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 8.1 – operatiivne planeerimine ja ohje: nõuab turvalise arenduse protsesside ja kontrollimeetmete lõimimist tegevustesse.

11.2 ISO/IEC 27002:2022 – kontrollimeetmed 8.25–8.28

11.2.1 Lisa A kontrollimeede 8.25 – turvaline arenduse elutsükkel: nõuab turvalisuse ametlikku kaasamist tarkvara kavandamisse ja arendusse.

11.2.2 Lisa A kontrollimeede 8.26 – rakendusturbe nõuded: nõuab turvalise programmeerimise ja turbe vastuvõtukriteeriumide määratlemist.

11.2.3 Lisa A kontrollimeede 8.27 – turvaline süsteemiarhitektuur ja tehnoloogiapõhimõtted: nõuab turvalise kavandamise põhimõtete rakendamist ja teadaolevate nõrkuste maandamist.

11.2.4 Lisa A kontrollimeede 8.28 – turvaline programmeerimine: nõuab turvalise programmeerimise põhimõtete rakendamist ja kontrolli.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3 kuni SA-15: sätestab struktureeritud rakendusturbe arendustavad, sealhulgas nõuded kavandamisele, koodi terviklusele ja testimisele.

11.3.2 SI-10 – sisendi valideerimine: käsitleb turvalise programmeerimise kaitsemeetmeid.

11.3.3 SR-3 – tarneahela kaitse: nõuab kolmandate osapoolte tarkvara, komponentide ja arendusteenuse osutajate hindamist.

11.4 EL GDPR (2016/679)

11.4.1 Artikkel 25 – andmekaitse kavandamisel ja vaikimisi: nõuab turvalisuse ja andmekaitse lõimimist süsteemiarendusse.

11.4.2 Artikkel 32 – töötlemise turvalisus: toetab tehnilisi meetmeid, nagu sisendi valideerimine, juurdepääsukontroll ja turvaline juurutamine.

11.5 EL NIS2 direktiiv (2022/2555)

11.5.1 Artikkel 21(2)(e–f): nõuab tarkvaraarenduse tavasid, mis hõlmavad haavatavuste haldust, koodi turvet ja intsidentidest teatamist.

11.6 EL DORA (2022/2554)

11.6.1 Artikkel 9 – IKT-riskide juhtimine: nõuab finantssektori üksustele turvalise arenduse tavasid, sealhulgas tarkvara kvaliteedi kontrollimeetmeid ja puuduste kõrvaldamist.

11.6.2 Artikkel 10 – talitluspidevus ja testimine: soodustab IKT-süsteemide, sealhulgas rakenduste, ranget testimist ja valideerimist.

11.7 COBIT 2019

11.7.1 BAI03 – lahenduste tuvastamise ja ehitamise juhtimine: reguleerib kavandamist, arendust ja turvalisuse lõimimist uutesse lahendustesse.

11.7.2 BAI07 – muudatuste vastuvõtmise ja ülemineku juhtimine: tagab turvalise juurutamise ja juurutusjärgse hindamise.

11.7.3 DSS05 – turbeteenuste juhtimine: kohaldab turbevalideerimist tarkvara ja teenuste osutamisele.