					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P24S					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**

Kooskõla standardite ja regulatsioonidega

Standard/õigusnorm	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 8	Asjakohased turbekontrollid tegevuspraktikate jaoks, sealhulgas turvaline arendus
ISO/IEC 27002:2022	Kontrollimeetmed 8.25–8.27	Hõlmab turvalist arenduse elutsüklit, testimist ja kolmandate osapoolte arendajate turbekohustusi
NIST SP 800-53 Rev.5	SA-3 – SA-15, SI-10	Käsitleb turvalist tarkvaraarenduse elutsüklit, juurdepääsukontrolli ja haavatavuste käsitlemist arenduses
EL GDPR	Artikkel 25	Nõuab tarkvaraarenduses lõimitud andmekaitset ja vaikimisi andmekaitset
EL NIS2	Artikkel 21(2)(a), (e), (h)	Kohustab kehtestama turvalise arenduse poliitikad, avatud lähtekoodi kasutuse järelevalve ja riskimaandamise dokumentatsiooni
EL DORA	Artikkel 6(7), 9(1)(c), 10(2)(c)	Elutsükli turvalisus finantssektori kriitiliste IKT-süsteemide jaoks
COBIT 2019	BAI	Raamistik struktureeritud, jälgitava ja toimepideva turvalise arenduse juhtimiseks

1. Eesmärk

1.1 Käesoleva poliitika eesmärk on tagada, et kogu organisatsiooni või selle väliste partnerite loodud või muudetud tarkvara, skriptid ja veebipõhised tööriistad arendatakse turvaliselt, vähendades haavatavuste, loata juurdepääsu andmetele ja töökatkestuste riski.

1.2 Käesolev poliitika määratleb kohustuslikud turvalise arenduse nõuded ja turvalise programmeerimise praktikad, mida peavad järgima kõik sisearendajad, töövõtjad ja tarnijad sõltumata projekti suurusest või keerukusest.

1.3 Käesoleva poliitika eesmärk on kaitsta kliendiandmeid, ennetada rikkumisi ning tagada, et organisatsiooni poolt või organisatsiooni jaoks loodud või kohandatud tarkvara on auditivalmis, vastab õiguslikele nõuetele (nt GDPR, NIS2, DORA) ja toetab ISO/IEC 27001 sertifitseerimist.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib kõigile isikutele ja üksustele, kes organisatsiooni nimel arendavad, kohandavad, juurutavad või haldavad järgmist:

2.1.1 veebisaidid, rakendused või automatiseerimisvahendid;

2.1.2 organisatsioonisiseselt arendatud skriptid või tarkvara;

2.1.3 kolmandate osapoolte arendajate või vabakutseliste loodud kood;

2.1.4 pluginad, teegid ja tarkvarakomponendid, mis on integreeritud tootmiskeskkonda.

2.2 See hõlmab kõiki arendustegevustes kasutatavaid keskkondi, sealhulgas:

2.2.1 arendus- ja testkeskkonnad;

2.2.2 vahekeskkond ja eeltootmiskeskkond;

2.2.3 tootmissüsteemid, kus käivitatakse kohandatult arendatud koodi.

2.3 Poliitika reguleerib ka andmete töötlemist arenduse ja juurutamise käigus, eelkõige tootmisandmete kasutamist tootmisvälises keskkonnas.

3. Eesmärgid

3.1 Ennetada turvavigade või haavatavuste lisandumist kohandatud või kolmandate osapoolte arendatud tarkvarasse.

3.2 Tagada, et turvalise programmeerimise praktikad ja haavatavuste ennetamine on lõimitud tarkvaraarenduse elutsükli igasse etappi.

3.3 Vähendada avatud lähtekoodiga või kolmandate osapoolte komponentide kasutamisega seotud riske, nõudes asjakohast kontrolli ja seiret.

3.4 Nõuda ametlikku koodi läbivaatust ja rakenduse turbetestimist enne väljalaset.

3.5 Kontrollida juurdepääsu arenduskeskkondadele ja tagada nende eraldatus aktiivses kasutuses olevatest tootmissüsteemidest.

3.6 Täita rahvusvahelistest standarditest ja regulatsioonidest tulenevad kohustuslikud nõuded (nt ISO/IEC 27001, GDPR, DORA, NIS2).

4. Rollid ja vastutused

4.1 Tegevjuht

4.1.1 Kiidab käesoleva poliitika heaks ja vastutab selle rakendamise eest.

4.1.2 Tagab, et kogu tarkvaraarendus, nii organisatsioonisisene kui ka sisseostetud, vastab käesolevale poliitikale.

4.1.3 Vaatab läbi ja allkirjastab arendus- või teenuslepingud, mis sisaldavad turvalise arenduse nõudeid.

4.1.4 Kontrollib tarnijate vastavust regulaarsete ülevaatuste või turvalisust tõendava materjali küsimise kaudu.

4.2 Sisearendaja või rakenduse omanik

4.2.1 Järgib turvalise programmeerimise ja juurutamise praktikaid.

4.2.2 Rakendab igas projektis turvalise arenduse kontrollnimekirja.

4.2.3 Kontrollib kõigi kasutatavate avatud lähtekoodiga või kolmandate osapoolte komponentide turvalisust.

4.2.4 Teatab kõigist avastatud haavatavustest viivitamata tegevjuhile.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Tegevjuht peab käesoleva poliitika läbi vaatama vähemalt üks kord aastas, et:

9.1.1 kontrollida jätkuvat vastavust standarditele ISO/IEC 27001, GDPR, NIS2 ja DORA;

9.1.2 kajastada ajakohastatud ohte või muutusi turvalise arenduse parimates praktikates;

9.1.3 tagada ühilduvus uute tööriistade, platvormide või tarnijasuhetega.

9.2 Vaheülevaatused tuleb algatada järgmistel juhtudel:

9.2.1 mis tahes teatatud tarkvara turbeintsident;

9.2.2 uue arendusraamistiku või majutusplatvormi kasutuselevõtt;

9.2.3 muudatus kolmandatest osapooltest arenduspartnerites;

9.2.4 regulatiivsed muudatused, mis mõjutavad tarkvara või turbekohustusi.

9.3 Kõik selle poliitika muudatused peavad olema:

9.3.1 dokumenteeritud kuupäeva, muudatuse kokkuvõtte ja tegevjuhi heakskiiduga;

9.3.2 selgelt edastatud kõigile sise- ja välistele arendusega seotud töötajatele;

9.3.3 säilitatud osana organisatsiooni poliitika versioonihaldusest ja muudatuste ajaloost.

9.4 Uuendatud versioonid peavad olema hõlpsasti kättesaadavad kas siseplatvormide, trükitud dokumentatsiooni või tarnijatele ligipääsetavate pilveteenuste kaudu.

10. Seotud poliitikad ja seosed

10.1 Käesolev poliitika toetab mitme muu VKE poliitika rakendamist ja sõltub neist:

10.1.1 P2S – Juhtimisrollide ja vastutuste poliitika: kehtestab vastutuse arenduse turbekontrollide määramise ja kontrollimise eest projektide ja tarnijate lõikes.

10.1.2 P4S – Juurdepääsukontrolli poliitika: sätestab baaseeskirjad arenduskeskkondadele ja koodirepositooriumidele juurdepääsu piiramiseks, sealhulgas ülesannete lahususe.

10.1.3 P8S – Infoturbeteadlikkuse koolituse poliitika: tagab, et sisearendajad ja töövõtjad mõistavad turvalise programmeerimise praktikaid ja nendega seotud turbekohustusi.

10.1.4 P17S – Andmekaitse ja privaatsuse poliitika: selgitab, kuidas isikuandmeid tuleb arenduse, testimise ja logimise käigus töödelda, et tagada GDPR-i nõuetele vastavus.

10.1.5 P30S – Intsidentidele reageerimise poliitika: määratleb, kuidas arendusega seotud turbeintsidentidest tuleb teatada, neid hinnata ja kõrvaldada, sealhulgas koodiga seotud kokkupuuteid.

10.2 Kõik need poliitikad toimivad koos, et tagada turvalise arenduse rakendatavus ja tõendatavus ka väikeses või mittetehnilises organisatsioonis.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 8.1 – nõuab tegevuskontrollide, sealhulgas turvalise arenduse, rakendamist viisil, mis on kooskõlas ärieesmärkide ja riskipositsiooniga.

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.25 – soovitab lõimida turvalisuse kogu tarkvara elutsüklisse, sealhulgas lähtekoodi haldusse, versioonihaldusse ja arendajate juurdepääsu haldusse.

11.2.2 Kontroll 8.26 – määrab rakenduste testimise meetodid ja turvafunktsioonide verifitseerimise enne tootmiskeskkonda viimist.

11.2.3 Kontroll 8.27 – nõuab, et kolmandate osapoolte arendajad järgiksid samu arendusstandardeid ning et nende turbekohustused oleksid selgelt määratletud.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3 kuni SA-15 – määratlevad turvalise arenduse protsessid, sealhulgas arendajate juurdepääsukontrolli, testimise, ohumudeldamise ja dokumentatsiooni.

11.3.2 SI-10 – nõuab, et arendajad tuvastaksid ja maandaksid levinud tarkvara nõrkusi ning kasutaksid vajaduse korral automatiseeritud tööriistu.

11.4 EL GDPR (2016/679)

11.4.1 Artikkel 25 – „andmekaitse lõimitult ja vaikimisi“ kohustab lõimima turvalisuse ja andmekaitse tarkvara kavandamisse ja arendusse, eriti juhul, kui töödeldakse isikuandmeid.

11.5 EL NIS2 direktiiv (2022/2555)

11.5.1 Artikkel 21(2)(a), (e) ja (h) – nõuab turvalise arenduse poliitikaid, avatud lähtekoodi kasutuse järelevalvet ning rakendustega seotud riskide dokumenteeritud maandamist olulistes ja tähtsates üksustes.

11.6 EL DORA (2022/2554)

11.6.1 Artiklid 6(7), 9(1)(c) ja 10(2)(c) – kehtestavad finantssektori üksustele, sealhulgas VKE-dele, arenduse elutsükli turvalisuse kohustused, eelkõige kriitiliste IKT-süsteemide puhul.

11.7 COBIT 2019

11.7.1 BAI03 – „Lahenduste tuvastamise ja ülesehitamise juhtimine“ toetab struktureeritud arenduskontrollide rakendamist, rõhutades turvalisust, jälgitavust ja toimepidevust ning arvestades VKE-de piiranguid.