					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P28					Dokumendi pealkiri: **Allhankearenduse 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**

Õiguslik teatis (autoriõigus ja kasutuspiirangud)

(C) 2025 Clarysec LLC. All rights reserved.

Käesolev dokument on Clarysec LLC intellektuaalomand. Selle dokumendi ühtegi osa ei tohi ilma eelneva selgesõnalise kirjaliku loata kopeerida, taaskasutada, levitada ega muuta ärilistel või rakendamise eesmärkidel.

Loata kasutamine on rangelt keelatud ja võib kaasa tuua õiguslikke meetmeid.

Litsentsimise küsimustes võtke ühendust: info@clarysec.com

Kooskõla standardite ja õigusaktidega

Standard/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 8.1	Ei kohaldu
ISO/IEC 27002:2022	Kontrollimeetmed 5.19-5.22, 8	Ei kohaldu
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-10	Ei kohaldu
EL isikuandmete kaitse üldmäärus (GDPR)	Artiklid 28, 32	Ei kohaldu
EL NIS2 direktiiv	Artiklid 21(2)(a), (h), 23	Ei kohaldu
EL DORA määrus	Artiklid 28(1), (2)	Ei kohaldu
COBIT 2019	APO10, BAI03, DSS	Ei kohaldu

1. Eesmärk

1.1 Käesolev poliitika kehtestab kohustuslikud kontrollimeetmed tarkvara- või süsteemiarenduse allhankimisel välistele tarnijatele, töövõtjatele või agentuuridele, et turvalised praktikad oleksid lõimitud kogu arenduse elutsükli vältel.

1.2 Selle eesmärk on ennetada haavatavusi, andmekadu, intellektuaalomandi (IP) loata avalikustamist ning vastavusnõuete rikkumisi, mis tulenevad väliste arendajate kaasamisest.

1.3 Poliitika sätestab tarnijahalduse, turvalise programmeerimise standardite, juurdepääsuhalduse, seirekohustuste ning lepingu lõppemisega seotud väljumisprotsessi nõuded, et tagada arendatava tarkvara konfidentsiaalsus, terviklus ja käideldavus.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub kõigile organisatsiooni üksustele, kes kaasavad tarkvara- või süsteemiarendusse väliseid osapooli, sealhulgas:

2.1.1 veebirakendused, mobiilirakendused, manussüsteemid, API-d, skriptid, automatiseeritud töövood või platvormimoodulid

2.1.2 sisemiste platvormide, kliendisuunatud süsteemide või kommertstoodete kohandusarendus

2.1.3 projektid, millesse on kaasatud kolmandate osapoolte arendajad, vabakutselised, agentuurid või välisriikides asuvad meeskonnad

2.2 Käesolev poliitika kohaldub ka kõigile välistele osapooltele, kellel on arenduse käigus juurdepääs lähtekoodile, testkeskkondadele või CI/CD torustikele.

2.3 Käesoleva poliitika nõuete täitmine on kohustuslik sõltumata lepingu tüübist, arendusmetoodikast või allhanketeenuse osutaja geograafilisest asukohast.

3. Eesmärgid

3.1 Rakendada turvalise arenduse elutsükli (SDLC) praktikaid kõigis allhankearenduse projektides alates planeerimisest kuni kasutuselevõtujärgse valideerimiseni.

3.2 Tagada, et kõik väliste arendajatega sõlmitavad lepingud sisaldavad kohustuslikke sätteid andmekaitse, turvalise programmeerimise ja intellektuaalomandi õiguste säilimise kohta.

3.3 Määratleda juurdepääsuhalduse, seire ja auditi nõuded kolmandate osapoolte arendajatele, kes kasutavad sisemisi süsteeme.

3.4 Kaitsta organisatsiooni tarneahela ohtude, õigusaktide rikkumiste ja väliselt arendatud tarkvaraga seotud mainekahju eest.

3.5 Tagada pidev vastavus turberaamistike nõuetele, sealhulgas ISO/IEC 27001, NIST, GDPR, NIS2, DORA ja COBIT 2019.

4. Rollid ja vastutused

4.1 Tippjuhtkond

4.1.1 Kiidab heaks kõrge riskiga allhankearenduse projektid ja kinnitab põhjendatud poliitikaerandid.

4.1.2 Tagab, et allhankeotsused on kooskõlas strateegiliste eesmärkide ja organisatsiooni riskivalmidusega.

4.2 Infoturbejuht (CISO)

4.2.1 Kiidab infoturbe seisukohast heaks tarnija kaasamise protsessi.

4.2.2 Määratleb allhankeprojektide turbekontrollide nõuded ja vaatab läbi intsidentiaruanded.

[... 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 järgmistel asjaoludel:

9.1.1 uute allhankearenduse mudelite, tarnijate või jurisdiktsioonide kasutuselevõtt

9.1.2 muudatused regulatiivsetes nõuetes, näiteks GDPR-is, NIS2-s või DORAs

9.1.3 pärast allhankearenduse lähtekoodi, juurdepääsu või töötulemitega seotud turbeintsidenti

9.1.4 siseauditi leidude või infoturbe juhtimissüsteemi (ISMS) täiustamise tulemusel

9.2 Infoturbejuht (CISO) vastutab poliitika läbivaatamise algatamise ja koordineerimise eest, konsulteerides järgmiste osapooltega:

9.2.1.1 hanke- ja õigusmeeskonnad (lepinguliste nõuete rakendamise kooskõlastamiseks)

9.2.1.2 projektiomanikud ja tooteomanikud (operatiivse teostatavuse hindamiseks)

9.2.1.3 infoturbemeeskond (ohtude ja kontrollimeetmete ajakohastamiseks)

9.2.1.4 tippjuhtkond (lõpliku heakskiidu andmiseks)

9.3 Kõik poliitikamuudatused peavad olema:

9.3.1.1 kajastatud versioonihalduses ja talletatud määratud dokumendihoidlas

9.3.1.2 teatatud sidusrühmadele, kes osalevad allhankearenduse tegevustes

9.3.1.3 seostatud seotud poliitikate või protseduuridokumentatsiooni ajakohastustega

9.4 Iga poliitikaversiooniga peab kaasnema muudatuste logi, mis tagab muudatuste ja heakskiitude jälgitavuse.

10. Seotud poliitikad ja seosed

10.1 Käesolev poliitika toetub järgmistele seotud dokumentidele ja toetab neid omakorda:

10.1.1 P1 - Infoturbepoliitika: kehtestab organisatsiooniülesed turbepõhimõtted, mis kehtivad nii sisemisele arendusele kui ka kolmandate osapoolte arendusele.

10.1.2 P5 - Muudatuste haldamise poliitika: tagab, et kõik allhankearenduse koodibaasidest tulenevad juurutamisega seotud muudatused vaadatakse läbi ja kiidetakse heaks enne rakendamist.

10.1.3 P13 - Andmete klassifitseerimise ja märgistamise poliitika: määrab kindlaks, kuidas tundlik teave tuvastatakse enne selle edastamist arendustarnijatele või repositooriumidesse.

10.1.4 P18 - Krüptograafiliste kontrollimeetmete poliitika: annab suunised, kuidas võtmeid, salajasi väärtusi ja tundlikke autentimistunnuseid tuleb arenduse ja üleandmise käigus käidelda.

10.1.5 P24 - Turvalise arenduse poliitika: määratleb sisemise ja välise tarkvaraarenduse praktikate miinimumnõuded.

10.1.6 P30 - Intsidentidele reageerimise poliitika: reguleerib, kuidas allhankearendusega seotud rikkumisi või turbeprobleeme eskaleeritakse, uuritakse ja lahendatakse.

10.1.7 P33 - Auditi ja vastavuse seire poliitika: määrab nõuded allhankearenduse tegevuste läbivaatamiseks auditite või vastavuse ülevaatuste käigus.

11. Viitestandardid ja -raamistikud

11.1 Käesolev poliitika on kooskõlas rahvusvaheliselt tunnustatud turberaamistike ja õigusaktidega, et tagada tarkvaraarenduse turvaline allhange ja tõhus tarnijahaldus.

11.2 ISO/IEC 27001

11.2.1 Punkt 8.1 - Tegevuse planeerimine ja ohjamine: kehtestab protsessilised kontrollimeetmed turvalise arenduse ja kolmandate osapoolte osutatava arenduse jaoks.

11.3 ISO/IEC 27002:2022 - Kontrollimeetmed 5.19 kuni 5.21 ja 8.27.

11.3.1 Lisa A kontroll 5.19 - tarnijasuhete juhtimine: nõuab ametlikke lepinguid turbe- ja vastavussätetega.

11.3.2 Lisa A kontroll 5.20 - infoturbe käsitlemine tarnijalepingutes: tagab, et arendusega seotud kontrollimeetmed on lepingutesse lisatud.

11.3.3 Lisa A kontroll 5.21 - tarnijate teenuse osutamise juhtimine: hõlmab kolmandate osapoolte arenduse töötulemuste ja riskide seiret.

11.3.4 Lisa A kontroll 8.27 - allhankearendus: nõuab väliselt arendatud tarkvara puhul määratletud turbenõudeid ja juurdepääsukontrolli.

11.3.5 Need kontrollimeetmed kehtestavad struktureeritud nõuded allhankearendajate valikuks, lepingute sõlmimiseks ja järelevalveks, sealhulgas turvalise arenduse praktikad, lähtekoodi käitlemine ja tulemuslikkuse valideerimine.

11.4 NIST SP 800-53 Rev.5

11.4.1 SA-4 - hankeprotsess: nõuab, et turvalise arenduse nõuded oleksid määratletud hanke käigus.

11.4.2 SA-9 - välised süsteemiteenused: reguleerib, kuidas kolmandate osapoolte arendajad saavad sisemisi teenuseid turvaliselt kasutada.

11.4.3 SA-10 - arendaja konfiguratsioonihaldus: on kooskõlas väliste meeskondade versioonihalduse, lähtekoodile juurdepääsu ja muudatuste jälgimise kohustustega.

11.5 EL isikuandmete kaitse üldmäärus (GDPR) (2016/679)

11.5.1 Artikkel 28 - volitatud töötleja kohustused: nõuab, et kolmandate osapoolte arendajatega sõlmitud lepingutes oleksid isikuandmete töötlemise turbe-, kontrolli- ja auditeerimisnõuded selgelt määratletud.

11.5.2 Artikkel 32 - töötlemise turvalisus: nõuab asjakohaste kaitsemeetmete (nt krüptimine, juurdepääsukontroll) rakendamist isikuandmeid töötlevate süsteemide arendamisel.

11.6 EL NIS2 direktiiv (2022/2555)

11.6.1 Artiklid 21(2)(a), (h), 23: nõuavad turvalise arenduse praktikate rakendamist kolmandate osapoolte kaasamisel ja digitaalses tarneahelas koos järelevalve ja tehniliste kontrollimeetmetega.

11.7 EL DORA määrus (2022/2554)

11.7.1 Artiklid 28(1), (2): nõuavad, et finantssektori üksused juhiksid kolmanda osapoole IKT-riske lepinguliste kontrollimeetmete ja turvalise arenduse järelevalve kaudu, eriti kriitilise allhankearenduse korral.

11.8 COBIT 2019

11.8.1 APO10 - tarnijate juhtimine: kehtestab struktureeritud nõuded tarnijate hindamiseks, lepingute sõlmimiseks ja tulemuslikkuse seireks.

11.8.2 BAI03 - lahenduste arendamise juhtimine: vastab otseselt turvalise arenduse elutsükli protsessidele, koodiläbivaatustele ja arenduse valideerimisele.

11.8.3 DSS05 - turvateenuste juhtimine: on kooskõlas väliselt arendatud süsteemide seire ja kaitsega.