| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sisestage siia registreeritud juriidilise isiku nimi | | | | | | | |
| Dokumendi number:<br>P28S | | | | | Dokumendi pealkiri:<br>**Allhankearenduse poliitika** | | | | | | | |
| Versioon:<br>1.0 | | Jõustumiskuupäev:<br>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 | Punktid 5.1, 6.1, 8 | Kohaldatavad ISMSi ja tarnijatega seotud ohjemeetmed |
| ISO/IEC 27002:2022 | Ohjemeetmed 5.19, 5.20, 8.25–8.27 | Tarnijate ja turvalise arenduse elutsükli ohjemeetmed |
| NIST SP 800-53 Rev. 5 | SA-4, SA-9, SA-11, SA-15, SR-3 | Hanke, tarneahela, turvalise arenduse ja tarnijalepingute nõuded |
| ELi isikuandmete kaitse üldmäärus (GDPR) | Artikkel 28 | Lepingulised ja andmekaitsenõuded kolmandate osapoolte isikuandmete töötlemisele |
| ELi NIS2 direktiiv | Artikkel 21(2)(a), (h) | Tarneahela ja turvalise rakendusarenduse ohjemeetmed |
| ELi DORA määrus | Artikkel 10 | IKT kolmandate osapoolte riskijuhtimine, sh allhankearendus |
| COBIT 2019 | BAI03, DSS05 | Nõuded välisarendusele ja välistele IT-teenuse osutajatele |

**1. Eesmärk**

1.1 Käesoleva poliitika eesmärk on tagada, et kogu allhankekorras tarkvaraarendus, olenemata sellest, kas seda teostavad vabakutselised, arendusagentuurid või muud kolmandatest osapooltest teenuseosutajad, toimub turvaliselt, on lepinguliselt reguleeritud ning vastab kohaldatavatele õigus-, regulatiivsetele ja auditinõuetele.

1.2 Käesolev poliitika kaitseb organisatsiooni ebaturvalise koodi, ebaselge omandiõiguse, andmete avalikustamise ja puuduliku tarnijahaldusega seotud riskide eest, kehtestades siduvad arendusstandardid ja teenuseosutajate järelevalve ka juhul, kui organisatsioonil puudub eraldi IT-osakond.

1.3 Käesolev poliitika toetab ISO/IEC 27001:2022 sertifitseerimist, määratledes selged ootused arendusele, vastutusele ja dokumenteeritud ohjemeetmetele kolmandate osapoolte arendustegevuses.

**2. Kohaldamisala**

**2.1 Käesolev poliitika kehtib järgmistele osapooltele ja tegevustele:**

2.1.1 kõik allhankearendajad, sealhulgas vabakutselised ja arendusagentuurid;

2.1.2 kõik arendustööd, mis hõlmavad sisemisi tööriistu, avalikult kättesaadavaid veebisaite, tarkvararakendusi või äriprotsesside automatiseerimist;

2.1.3 töötajad, kes vastutavad väliste arendajate valiku, juhtimise või järelevalve eest;

2.1.4 mis tahes kolmanda osapoole süsteemiintegratsioon, skriptimine või arendus, mis on liidestatud ettevõtte andmete või süsteemidega.

2.2 Poliitika hõlmab ka kõiki osapooli ja platvorme, millel on juurdepääs ettevõtte autentimisandmetele, andmehoidlatele, lähtekoodirepositooriumidele, testkeskkondadele või tootmissüsteemidele.

**3. Eesmärgid**

3.1 Tagada, et kogu allhankearendus järgib turvalise programmeerimise põhimõtteid ning et arendajad on lepinguliselt kohustatud järgima dokumenteeritud standardeid ja konfidentsiaalsuslepingu (NDA) tingimusi.

3.2 Kehtestada omandiõigus kõigi väljundite üle, sealhulgas kood, varad, autentimisandmed ja dokumentatsioon, tagades õiguste täieliku üleandmise ettevõttele ning jälgitava üleandmise projekti lõppemisel.

3.3 Ennetada levinud arendusriske, sealhulgas omandilise koodi korduskasutust, teekide kaudu toimuvaid tarneahela ründeid, toeta raamistike kasutamist ja kontrollimata haldusjuurdepääsu.

3.4 Nõuda iga allhankeprojekti puhul enne töö alustamist dokumentatsiooni olemasolu, sealhulgas lepinguid, konfidentsiaalsuslepinguid (NDA-sid) ja minimaalseid turbenõudeid.

3.5 Kaitsta kliendiandmeid, süsteeme ja sisemisi protsesse, tagades tõhusa arenduse järelevalve, tarnejärgse testimise ja süsteemidele juurdepääsu turvalise halduse.

**4. Rollid ja vastutused**

**4.1 Tegevjuht**

4.1.1 Kiidab heaks kõik tarnijasuhted ja allkirjastab arenduslepingud.

4.1.2 Tagab, et kogu allhankearendus vastab käesolevale poliitikale.

4.1.3 Tagab juurdepääsude eemaldamise ettevõtte süsteemidele pärast projekti lõppemist.

4.1.4 Vaatab läbi tarnejärgse dokumentatsiooni ja tulemused.

**4.2 Projekti omanik (tavaliselt sisemine töötaja või määratud koordinaator)**

4.2.1 Korraldab igapäevast koordineerimist välise arendajaga.

4.2.2 Kontrollib, et funktsionaalsed nõuded on täidetud ja väljundid on testitud.

4.2.3 Tagab koodi ja autentimisandmete turvalise üleandmise.

4.2.4 Teatab tegevjuhile kõigist arendusega seotud probleemidest või turvaintsidentidest.

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

**9. Läbivaatamise ja ajakohastamise nõuded**

**9.1 Iga-aastane läbivaatamine**

**9.1.1 Tegevjuht peab käesoleva poliitika läbi vaatama vähemalt kord aastas. Läbivaatamise eesmärk on tagada, et poliitika vastab jätkuvalt järgmistele nõuetele:**

9.1.1.1 ISO/IEC 27001 sertifitseerimisnõuded;

9.1.1.2 õiguslike kohustuste muudatused (nt GDPR artikkel 28, DORA artikkel 10);

9.1.1.3 VKE tasemele vastavad arenduspraktikad ja kolmandate osapoolte riskid.

**9.2 Vahepealsed läbivaatused**

**9.2.1 Poliitika tuleb läbi vaadata ka siis, kui:**

9.2.1.1 kaasatakse uus allhankearenduse tarnija või platvorm;

9.2.1.2 toimub oluline allhankearendusega seotud intsident;

9.2.1.3 kasutatavates tööriistades, platvormides või keskkondades toimuvad olulised muudatused.

**9.3 Läbivaatamise protsess**

**9.3.1 Tegevjuht vastutab järgmise eest:**

9.3.1.1 kontrollib, et lepingud, konfidentsiaalsuslepingud (NDA-d) ja juurdepääsukontrolli protsessid on jätkuvalt tõhusad;

9.3.1.2 kinnitab, et praegused tarnijad ja vabakutselised tegutsevad kooskõlas poliitikaga;

9.3.1.3 ajakohastab tingimusi varasemate projektide või intsidentide tagasiside põhjal.

**9.4 Versioonihaldus ja teavitamine**

**9.4.1 Kõik muudatused peavad olema:**

9.4.1.1 registreeritud koos kuupäeva, põhjuse ja muudatuse kirjeldusega;

9.4.1.2 tegevjuhi poolt heaks kiidetud ja lisatud versiooniajalukku;

9.4.1.3 edastatud kõigile töötajatele või projektiomanikele, kes töötavad väliste arendajatega;

9.4.1.4 vajaduse korral edastatud ka kõigile mõjutatud tarnijatele ja kolmandatele osapooltele.

**10. Seotud poliitikad ja seosed**

**10.1 Käesolev poliitika toetab otseselt järgmiste VKE-le kohandatud poliitikate rakendamist ja sõltub neist:**

10.1.1 P2S – Juhtimisrollide ja vastutuste poliitika: täpsustab, kes vastutab tarnijate heakskiitmise, juurdepääsukontrolli ja riski aktsepteerimise eest allhankearendajate kasutamisel.

10.1.2 P4S – Juurdepääsukontrolli poliitika: määratleb allhankearenduse käigus kasutatavate kasutajakontode ja administraatoriõigustega juurdepääsu korrektse loomise, piiramise ja lõpetamise.

10.1.3 P8S – Infoturbeteadlikkuse ja koolituse poliitika: tagab, et sisemised töötajad mõistavad, kuidas väliste arendajatega turvaliselt koordineerida, sealhulgas autentimisandmete ja projektifailide käsitlemist.

10.1.4 P17S – Andmekaitse ja privaatsuspoliitika: kehtestab turbe- ja õigusnõuded isikuandmete töötlemiseks, millele allhankearendajad võivad GDPRi alusel juurde pääseda või mida nad võivad töödelda.

10.1.5 P24S – Turvalise arenduse poliitika: määratleb, kuidas sisemine ja väline arendus peab järgima turvalise programmeerimise tavasid ning teekide ja raamistike kontrolli.

10.1.6 P30S – Intsidentidele reageerimise poliitika: kohaldub juhul, kui allhankearendus põhjustab turvaintsidente või haavatavusi, ning suunab koordineeritud uurimist ja puuduste kõrvaldamist.

10.2 Neid poliitikaid tuleb rakendada paralleelselt, et allhankearendus ei tekitaks juhtimata riske ega põhjustaks VKE vastavuskohustuste rikkumist.

**11. Viitestandardid ja raamistikud**

**11.1 ISO/IEC 27001**

11.1.1 Punkt 6.1 – Organisatsioonid peavad hindama ja käsitlema tarnijatega seotud infoturberiske.

11.1.2 Punkt 8.1 – Nõuab tegevuste planeerimist ja ohjet, sealhulgas kolmandate osapoolte teenuste, näiteks allhankearenduse, puhul.

**11.2 ISO/IEC 27002**

11.2.1 Ohjemeede 5.19 – Soovitab hinnata tarnijate suutlikkust täita infoturbenõudeid.

11.2.2 Ohjemeede 5.20 – Soovitab kolmandate osapoolte teenuste korrapärast seiret ja perioodilist läbivaatamist.

11.2.3 Ohjemeetmed 8.25–8.27 – Kirjeldavad turvalise arenduse elutsükli praktikaid, mida saab kohaldada allhankearendusele.

**11.3 NIST SP 800-53 Rev. 5**

11.3.1 SA-4 – Nõuab, et hankestrateegiad sisaldaksid infoturbemeetmeid.

11.3.2 SA-9 – Käsitleb väliste süsteemide arendust ja tarneahela riske.

11.3.3 SA-11 – Määratleb turvalise arenduse praktikad, sealhulgas koodi läbivaatuse ja puuduste kõrvaldamise.

11.3.4 SA-15 – Soovitab kasutada puuduste tuvastamiseks ja tarkvara usaldusväärsuse tagamiseks automatiseeritud tööriistu.

11.3.5 SR-3 – Nõuab, et tarnijalepingud sisaldaksid küberturbenõudeid.

**11.4 Euroopa Liidu isikuandmete kaitse üldmäärus (GDPR)**

11.4.1 Artikkel 28 – Nõuab lepinguid kolmandatest osapooltest volitatud töötlejatega, et tagada asjakohased andmekaitsemeetmed; see on otseselt kohaldatav arendajatele, kes töötlevad isikuandmeid või kellel on neile juurdepääs.

**11.5 ELi NIS2 direktiiv (2022/2555)**

11.5.1 Artikkel 21(2)(a), (h) – Nõuab tarneahela turbeohjemeetmete ja turvalise tarkvaraarenduse praktikate rakendamist kohaldamisalasse kuuluvatele digitaalteenuse osutajatele, sealhulgas vajaduse korral VKEdele.

**11.6 ELi digitaalne tegevuskerksuse määrus (DORA)**

11.6.1 Artikkel 10 – Nõuab IKT kolmandate osapoolte riskijuhtimist, sealhulgas arenduslepinguid, turbekohustusi ja riskiohjemeetmeid, mis on seotud kolmandate osapoolte teenuseosutajatega.

**11.7 COBIT 2019**

11.7.1 BAI03 – Lahenduste tuvastamise ja loomise juhtimine – tagab, et väline arendus vastab ärinõuetele ja turbeootustele.

11.7.2 DSS05 – Turvateenuste juhtimine – nõuab, et välised turvateenused ja arendusteenuse osutajad tegutseksid kehtestatud turbereeglite ja järelevalve alusel.