					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P26S					Dokumendi pealkiri: **Kolmandate osapoolte ja tarnijate turbepoliitika**							
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/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 8	Operatiivsed kontrollimeetmed kolmandate osapoolte ja tarnijatega seotud suhete jaoks
ISO/IEC 27002:2022	Kontrollimeetmed 5.19–5.22	Tarnijate turvakontrollid, lepingulised turbetingimused, muudatuste juhtimine, seire ja läbivaatamine
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Hanked, konfiguratsioon, ühenduslepingud ja välise personali kontrollimeetmed
ELi isikuandmete kaitse üldmäärus (GDPR)	Artiklid 28, 32	Andmetöötluslepingud, volitatud töötlejate turbega seotud nõuded
ELi NIS2	Artiklid 21(2)(a)(b)(i), 23(1)	Tarneahela riskijuhtimine, kolmandate osapoolte teenuste järelevalve
ELi DORA	Artiklid 5(1)(2), 28(1)(2)	IKT-riskide juhtimine kolmandatest osapooltest teenuseosutajate puhul
COBIT 2019	APO10, APO12, DSS05	Tarnijahaldus ja riskide lõimimine

1. Eesmärk

1.1 Käesolev poliitika kehtestab kohustuslikud turbenõuded suhete loomiseks, haldamiseks ja lõpetamiseks kolmandate osapoolte ja tarnijatega, kellel on juurdepääs organisatsiooni andmetele, süsteemidele või teenustele või kes mõjutavad neid.

1.2 Sellega tagatakse, et välised teenuseosutajad, sealhulgas IT-tugiteenuse osutajad, pilveteenuse pakkujad, tarkvaraarendajad ja äriprotsesse toetavad töövõtjad, käitlevad ettevõtte varasid turvaliselt ning kooskõlas kohaldatavate õigusaktide ja standarditega.

1.3 Käesolev poliitika vähendab riske, nagu andmelekked, süsteemides tehtavad loata muudatused, regulatiivsed trahvid või ebaturvalistest või ebapiisavalt juhitud kolmandate osapoolte kokkulepetest põhjustatud tegevushäired.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib kõikidele kolmandatele osapooltele, kes:

2.1.1 osutavad tarkvara-, taristu-, majutus- või pilveteenuseid;

2.1.2 kasutavad või haldavad sisemisi süsteeme, seadmeid või rakendusi;

2.1.3 käitlevad ettevõtte andmeid, dokumente või varukoopiaid;

2.1.4 toetavad äritegevust, personalivaldkonda (HR), finantsvaldkonda või klienditeenindust.

2.2 Käesolev poliitika kehtib ka järgmistele isikutele ja objektidele:

2.2.1 sisetöötajad, kes osalevad tarnijate valikus, kaasamises või järelevalves;

2.2.2 kõik töötajad, kes haldavad tarnijate kaasamisprotsessi, lepinguid, juurdepääsu või läbivaatusi;

2.2.3 kõik süsteemid või protsessid, mis sõltuvad kolmandate osapoolte komponentidest või teenustest.

3. Eesmärgid

3.1 Tagada, et kõik tarnijad täidavad selgelt määratletud turbeootusi.

3.2 Nõuda, et tarnijalepingud sisaldaksid kohaldatavaid turbe-, andmekaitse- ja intsidendile reageerimise kohustusi.

3.3 Hinnata ja dokumenteerida tarnijatega seotud riskid enne lepingu sõlmimist või juurdepääsu andmist.

3.4 Rakendada kõrge riskiga või kriitiliste tarnijate suhtes regulaarseid läbivaatusi vastavuse kinnitamiseks.

3.5 Kehtestada ametlik protsess erandite haldamiseks, intsidentide haldamiseks ja lepingute ajakohastamiseks.

3.6 Toetada vastavust standardi ISO/IEC 27001:2022, GDPR-i, NIS2 ja DORA nõuetele, mis on seotud tarnijate haldamisega.

4. Rollid ja vastutused

4.1 Tegevjuht (GM)

4.1.1 Vastutab lõplikult tarnijate valiku ja turbenõuete täitmise eest.

4.1.2 Kinnitab tarnijatega seotud lepingud, erandid ja eskalatsioonid.

4.1.3 Teostab järelevalvet intsidendile reageerimise ja otsustamise üle olukordades, kus tarnija ei täida oma kohustusi.

4.2 IT-teenuse osutaja või sisemine turbekoordinaator

4.2.1 Hindab tarnijate taotletud tehnilist juurdepääsu.

4.2.2 Rakendab juurdepääsukontrolli reegleid, vaatab läbi logid ja kontrollib andmete turvalist käitlemist.

4.2.3 Vaatab asjakohasel juhul läbi turvakontrollide, sertifitseeringute või audititulemuste tõendusmaterjali.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Käesolev poliitika tuleb vähemalt kord aastas läbi vaadata tegevjuhi poolt IT-teenuse osutaja või tarnijahalduri osalusel.

9.2 Poliitika tuleb läbi vaadata ka järgmistel juhtudel:

9.2.1 pärast olulist muudatust õiguslikes, regulatiivsetes või lepingulistes kohustustes;

9.2.2 pärast tarnijaga seotud turbeintsidenti või auditileidu;

9.2.3 uute tarnijakategooriate kasutuselevõtul (nt kriitilised SaaS-platvormid).

9.3 Kõik ajakohastused peavad olema:

9.3.1 dokumenteeritud koos versiooniajaloo ja põhjendusega;

9.3.2 tegevjuhi poolt kinnitatud;

9.3.3 teatavaks tehtud asjakohastele sisetöötajatele ja tarnijahalduritele;

9.3.4 säilitatud koos varasemate versioonidega vastavalt poliitikale P14S – Andmete säilitamise ja kõrvaldamise poliitika.

10. Seotud poliitikad ja seosed

10.1 Käesoleva poliitika tõhusus sõltub koordineerimisest järgmiste VKE infoturbepoliitikatega:

10.1.1 P2S – Juhtimisrollide ja vastutuste poliitika: määrab vastutuse tarnijate järelevalve ja lepingutingimuste rakendamise eest.

10.1.2 P4S – Juurdepääsukontrolli poliitika: määrab juurdepääsu piiramise reeglid, mida tuleb rakendada, kui tarnijatele antakse süsteemidele juurdepääs.

10.1.3 P17S – Andmekaitse ja privaatsuspoliitika: tagab, et isikuandmeid käitlevad tarnijad järgivad andmekaitsepõhimõtteid ja õiguslikke nõudeid.

10.1.4 P14S – Andmete säilitamise ja kõrvaldamise poliitika: kehtib kõikidele andmetele ja kirjetele, mida tarnijatega jagatakse või mida tarnijad säilitavad, ning reguleerib turvalist kõrvaldamist pärast lepingu lõppemist.

10.1.5 P30S – Intsidendile reageerimise poliitika: määratleb, kuidas reageerida olukorras, kus tarnija põhjustab turbeintsidendi või on sellesse kaasatud, sealhulgas eskalatsiooni ja tõendusmaterjali käitlemise protseduurid.

10.2 Need poliitikad toimivad koos, et tagada tarnijariskide ohjamine kogu lepingu elutsükli jooksul.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 8.1 – nõuab operatiivsete kontrollimeetmete rakendamist, sealhulgas kolmandate osapoolte ja tarnijatega seotud suhetes kohaldatavaid kontrollimeetmeid.

11.2 ISO/IEC 27002

11.2.1 Kontroll 5.19 – tagab, et tarnijate turvameetmed on kooskõlas organisatsiooni nõuetega.

11.2.2 Kontroll 5.20 – nõuab ametlikke kokkuleppeid, mis hõlmavad turbetingimusi, vastutusi ja rikkumisega seotud kohustusi.

11.2.3 Kontroll 5.21 – ohjab tarnijate teenustes tehtavaid muudatusi, mis võivad mõjutada turvaseisundit.

11.2.4 Kontroll 5.22 – nõuab tarnijate teenuste ja vastavuse seiret ning läbivaatamist.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-9 – reguleerib väliste süsteemide ja teenuste hankimist, nõudes riskihindamisi ja selgelt määratletud ootusi.

11.3.2 SA-10 – ohjab konfiguratsiooni- ja muudatusprotseduure, mis puudutavad kolmandate osapoolte hallatavaid süsteeme.

11.3.3 CA-3 – nõuab ühenduslepinguid süsteemidele, mis hõlmavad väliseid üksusi.

11.3.4 PS-7 – määratleb välise personali kontrolli ja vastutuse nõuded.

11.4 ELi isikuandmete kaitse üldmäärus (GDPR) (2016/679)

11.4.1 Artikkel 28 – nõuab andmetöötluslepinguid tarnijatega, kes tegutsevad volitatud töötlejatena.

11.4.2 Artikkel 32 – kohustab kõiki volitatud töötlejaid rakendama asjakohaseid tehnilisi ja korralduslikke meetmeid.

11.5 ELi NIS2 direktiiv (2022/2555)

11.5.1 Artikkel 21(2)(a), (b), (i) – kohustab rakendama IKT tarneahela riskijuhtimist ja kolmandate osapoolte kontrollimeetmeid.

11.5.2 Artikkel 23(1) – nõuab elutähtsate ja oluliste üksuste puhul kolmandate osapoolte teenuste dokumenteeritud järelevalvet.

11.6 ELi DORA (2022/2554)

11.6.1 Artikkel 5(1) – nõuab IKT-riskide juhtimise raamistikku, mis hõlmab kõiki kriitilisi kolmandatest osapooltest teenuseosutajaid.

11.6.2 Artikkel 5(2) – sätestab IKT-teenuste sõltuvuste jaoks lepingulised ja operatiivsed kontrollimeetmed.

11.6.3 Artikkel 28(1), (2) – kehtestab finantssektori IKT kolmanda osapoole riskide järelevalve reeglid.

11.7 COBIT 2019

11.7.1 APO10 – „Manage Suppliers“ kirjeldab hankimise kontrollimeetmeid ja suhtehalduse ootusi.

11.7.2 APO12 – „Manage Risk“ lõimib tarnijariskid organisatsiooni riskijuhtimisse.

11.7.3 DSS05 – „Manage Security Services“ kohaldub hallatud kolmandate osapoolte ja allhanke korras osutatavate teenuste puhul.