					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P37S					Dokumendi pealkiri: **Õigus- ja regulatiivse vastavuse 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/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punktid 5.1, 6.1, 6.2, 8	
ISO/IEC 27002:2022	Kontroll 5	
NIST SP 800-53 Rev.5	PL-1, PL-2, PM-1, CA-1, AU-1	
ELi isikuandmete kaitse üldmäärus (GDPR)	Artikkel 5, 6, 32, 33	
ELi NIS2 direktiiv	Artikkel 21(2)(a), 21(2)(f), 23	
ELi DORA määrus	Artikkel 5(2), 9(1), 17	
COBIT 2019	APO12, APO13, DSS01	

1. Eesmärk

1.1 Käesolev poliitika määratleb organisatsiooni lähenemise õiguslike, regulatiivsete ja lepinguliste kohustuste tuvastamisele, täitmisele ja vastavuse tõendamisele.

1.2 Käesoleva poliitikaga kehtestatakse selged vastutused ja praktilised tegevused, et toetada ettevõtet vastavuskohustuste täitmisel, sealhulgas andmekaitsenõuete, küberturberaamistike, kliendilepingute ja sertifitseerimisstandardite osas.

1.3 Käesolev poliitika tagab, et ka eraldi vastavusmeeskonna puudumisel suudab ettevõte hoida oma tegevuse õiguslikult põhjendatuna, reageerida intsidentidele asjakohaselt ja säilitada auditivalmiduse.

1.4 Käesolev poliitika on vajalik ISO/IEC 27001:2022 sertifitseerimise toetamiseks ning klientide, regulaatorite ja partnerite ootuste täitmiseks.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub järgmistele isikutele ja valdkondadele:

2.1.1 Kõik töötajad, töövõtjad, vabakutselised ja kolmandatest osapooltest tarnijad.

2.1.2 Kõik teenused, tegevused, süsteemid ja andmetöötlustoimingud, mille puhul organisatsioon peab täitma õiguslikke või lepingulisi nõudeid.

2.1.3 Kõik asukohad ja seadmed, mida kasutatakse äriteabe töötlemiseks, sõltumata sellest, kas need asuvad kontoris, on kasutusel kaugtöös või paiknevad pilvekeskkonnas.

2.2 Poliitika hõlmab järgmist:

2.2.1 Andmekaitsealased õigusaktid, näiteks GDPR.

2.2.2 Küberturbealased õigusaktid, näiteks NIS2.

2.2.3 Valdkonnapõhised kohustused, kui need on kohaldatavad.

2.2.4 Kliendilepingud, konfidentsiaalsuslepingud (NDA) ja auditõigusi käsitlevad sätted.

2.2.5 Vabatahtlikud sertifitseerimised (nt ISO 27001) ja sisepoliitikad, mida tuleb vastavuse tagamiseks rakendada.

3. Eesmärgid

3.1 Kehtestada vastutus: määrata selge vastutus õiguslike, regulatiivsete ja lepinguliste kohustuste seire, ajakohastamise ja rakendamise eest.

3.2 Kaitsta ettevõtet: vähendada õigusnormide rikkumise, trahvide, andmekaitserikkumiste ja mainekahju riski.

3.3 Tagada auditivalmidus: säilitada kontrollitavad kirjed, mis tõendavad, kuidas organisatsioon täidab oma vastavuskohustusi.

3.4 Toetada poliitikate lõimimist: tagada, et õiguslikke ja regulatiivseid kohustusi rakendatakse järjepidevalt kõigis poliitikates ja protsessides.

3.5 Hallata erandeid läbipaistvalt: tagada, et kõik vastavuserandid on dokumenteeritud, põhjendatud ja heaks kiidetud, et vältida vastutusriskide tekkimist.

4. Rollid ja vastutused

4.1 Tegevjuht (GM)

4.1.1 Vastutab organisatsiooni õigusliku ja regulatiivse vastavuse eest tervikuna.

4.1.2 Peab vastavusregistrit ja tagab selle ajakohasuse.

4.1.3 Vaatab läbi kliendilepingud ning tagab, et konkreetsed kohustused on jälgitavad ja rakendatud.

4.1.4 Kiidab vastavuskohustuste erandid heaks ainult juhul, kui need on õiguslikult põhjendatud ja rakendatud on kompenseerivad kontrollimeetmed.

4.2 Välised nõustajad (nt õigus-, IT- või vastavusnõustajad)

4.2.1 Toetavad tegevjuhti kohaldatavate õigusaktide, sertifitseerimiste ja kohustuste tuvastamisel (nt GDPR, NIS2, ISO 27001).

4.2.2 Annavad juhiseid uute regulatsioonide või kehtivate õigusaktide muudatuste tõlgendamiseks.

4.2.3 Võivad toetada poliitikate ajakohastamist, auditite läbiviimist või rikkumistele reageerimist, kui sellega kaasneb õiguslik risk.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Planeeritud iga-aastane läbivaatamine

9.1.1 Tegevjuht peab käesoleva poliitika läbi vaatama iga 12 kuu järel.

9.1.2 Läbivaatamisel tuleb kinnitada järgmist:

9.1.2.1 vastavus kehtivale õiguslikule ja lepingulisele kontekstile

9.1.2.2 kliendilepingute ja teenuskohustuste korrektne kajastamine

9.1.2.3 kooskõla vastavusregistri ja teiste poliitikatega

9.2 Sündmuspõhised ajakohastamised

9.2.1 Viivitamatu läbivaatamine on nõutav, kui:

9.2.1.1 kohaldatavaks muutub uus õigusakt või regulatsioon (nt uus andmekaitsenõue)

9.2.1.2 klient lisab lepingusse keerukad vastavustingimused

9.2.1.3 toimub rikkumine või vastavusintsident

9.2.1.4 ettevõte laieneb reguleeritud turule või tegevusvaldkonda

9.3 Muudatuste heakskiitmine ja versioonihaldus

9.3.1 Kõik muudatused tuleb dokumenteerida, versioonistada ja lasta tegevjuhil heaks kiita.

9.3.2 Varasemaid versioone tuleb säilitada auditi ja õiguslike eesmärkide tarbeks.

9.4 Muudatustest teavitamine

9.4.1 Töötajaid ja töövõtjaid tuleb poliitikamuudatustest teavitada 5 tööpäeva jooksul pärast heakskiitmist.

9.4.2 Kõik mõjutatud tarnijad peavad enne teenuse osutamise jätkamist samuti kinnitama, et on ajakohastatud tingimustega tutvunud.

10. Seotud poliitikad ja seosed

10.1 Käesoleva poliitika rakendamist toetavad järgmised VKE poliitikad:

10.1.1 P3S – IT-vahendite lubatud kasutuse poliitika: aitab ennetada tegevusi, mis võivad rikkuda õiguslikke või lepingulisi tingimusi (nt volitamata failijagamine).

10.1.2 P8S – Infoturbeteadlikkuse koolituse poliitika: annab töötajatele teadmised vastavuskohustustest ja rikkumiste vältimisest.

10.1.3 P14S – Andmete säilitamise ja kõrvaldamise poliitika: tagab õiguspärased andmekäitlustavad kogu andmete elutsükli jooksul.

10.1.4 P17S – Andmekaitse ja privaatsuspoliitika: tagab GDPR-i ja kliendiandmete käitlemisega seotud nõuete täitmise.

10.1.5 P30S – Intsidentidele reageerimise poliitika: kirjeldab andmekaitserikkumistele või vastavustõrgetele reageerimist, sealhulgas teatamistähtaegu.

10.1.6 P36S – Sotsiaalmeedia ja väliskommunikatsiooni poliitika: tagab, et avalik suhtlus ei rikuks õiguslikke ega regulatiivseid kohustusi.

10.2 Iga seotud poliitika rakendab osa õigusliku vastavuse raamistikust ning neid tuleb kohaldada koostoimes.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 6.1 – Riskide ja võimaluste käsitlemise tegevused: hõlmab vastavusriske.

11.1.2 Punkt 8.1 – Tegevuse planeerimine ja ohje: nõuab selliste protsesside rakendamist, mis vastavad õiguslikele ja lepingulistele nõuetele.

11.2 ISO/IEC 27002

11.2.1 Kontroll 5.36 – suunab organisatsiooni pidama kohustuste üle arvestust ja tagama asjakohase reageerimise õiguslikele ning regulatiivsetele nõuetele.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – poliitika ja protseduurid: nõuab ametlikke vastavuspoliitikaid.

11.3.2 PM-1 – infoturbeprogrammi plaan: nõuab õigusliku vastavuse lõimimist turbetegevuste planeerimisse.

11.3.3 CA-1 – hindamine, autoriseerimine ja seire.

11.3.4 AU-1 – auditipoliitika: nõuab vastavuse tõendusmaterjali säilitamist.

11.4 ELi isikuandmete kaitse üldmäärus (GDPR)

11.4.1 Artikkel 5 – isikuandmete töötlemise põhimõtted, sealhulgas vastutuse põhimõte.

11.4.2 Artikkel 6 – töötlemise õiguslik alus.

11.4.3 Artikkel 32 – töötlemise turvalisus.

11.4.4 Artikkel 33 – rikkumisest teatamine 72 tunni jooksul.

11.5 ELi NIS2 direktiiv

11.5.1 Artikkel 21(2)(a) ja (f) – sisepoliitikad riski ja regulatiivse kontrolli jaoks.

11.5.2 Artikkel 23 – rakendamine ja sanktsioonid vastavustõrgete eest.

11.6 ELi DORA määrus

11.6.1 Artikkel 5(2) – IKT-riski juhtimise järelevalve.

11.6.2 Artikkel 9(1) – vastavuse sisemine juhtimine.

11.6.3 Artikkel 17 – lepingulised kokkulepped IKT-teenuse osutajatega.

11.7 COBIT 2019

11.7.1 APO12 – hallatud risk: tagab, et vastavusriske jälgitakse ja käsitletakse.

11.7.2 APO13 – hallatud turve: hõlmab regulatiivse ja lepingulise vastavuse riskipõhist rakendamist.

11.7.3 DSS01 – hallatud operatsioonid: nõuab tegevusvalmidust õiguslike kohustuste täitmiseks.