					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P37					Dokumendi pealkiri: **Õigusnormidele 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**

1. Eesmärk

1.1 Käesolev poliitika kehtestab kohustusliku raamistiku kõigi organisatsiooni infoturbe, andmekaitse ja tegevusfunktsioonidega seotud õiguslike, regulatiivsete ja lepinguliste kohustuste tuvastamiseks, haldamiseks ja täitmiseks.

1.2 Eesmärk on vältida mittevastavust, mis võib kaasa tuua trahve, õigusvastutust, tegevushäireid, mainekahju või järelevalveasutuse sekkumist.

1.3 Käesolev poliitika toetab vastavusnõuete lõimimist juhtimisse, riskijuhtimisse, tegevusprotsessidesse, projektide elutsüklitesse ja süsteemide kavandamisse.

1.4 Sellega tagatakse, et kõik asjakohased kohustused eri jurisdiktsioonide, tegevusvaldkondade ja regulatiivsete kohaldamisalade lõikes on organisatsioonis selgelt dokumenteeritud, hinnatud, seiratud ja rakendatud.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib kõigile osakondadele, funktsioonidele, äriüksustele ja isikutele, kes tegutsevad organisatsiooni nimel, sealhulgas:

2.1.1 alalised ja ajutised töötajad;

2.1.2 töövõtjad, konsultandid ja praktikandid;

2.1.3 kolmandatest isikutest tarnijad, volitatud töötlejad või partnerid, kes käitlevad organisatsiooni andmeid, süsteeme või regulatiivseid kohustusi;

2.1.4 kõik äriprotsessid, projektid või algatused, mille suhtes kohaldub õiguslik või regulatiivne järelevalve.

2.2 Käesoleva poliitika alusel juhitavad vastavusvaldkonnad hõlmavad muu hulgas järgmist:

2.2.1 infoturbe- ja küberturbealased kohustused (nt ISO/IEC 27001, NIS2, DORA);

2.2.2 andmekaitse ja eraelu puutumatust reguleerivad õigusaktid (nt GDPR, valdkonnapõhised andmekaitsealased seadused);

2.2.3 valdkondlikud regulatsioonid (nt finants-, meditsiini-, autotööstuse ja kaitsevaldkonnas);

2.2.4 lepingulised kohustused, mis tulenevad konfidentsiaalsuslepingutest (NDA), teenustasemelepingutest (SLA) või kolmandate isikutega sõlmitud andmetöötluslepingutest;

2.2.5 õiguslikud nõuded, mis on seotud intsidentidest teavitamise, õiguskaitseasutustega suhtlemise ja piiriüleste andmeedastustega.

3. Eesmärgid

3.1 Tagada, et kõik kohaldatavad seadused, õigusnormid, standardid ja lepingulised kohustused on kogu organisatsioonis tuvastatud, dokumenteeritud, tõlgendatud ja rakendatud.

3.2 Lõimida õiguslikud ja regulatiivsed nõuded organisatsiooni ISMSi, riskijuhtimisprotsessidesse, tarnijalepingutesse ning toodete ja teenuste kavandamisse.

3.3 Luua mehhanism regulatiivsete muudatuste ennetavaks seireks ning kontrollimeetmete ja dokumentatsiooni ajakohastamiseks.

3.4 Määratleda selge vastutus vastavuse järelevalve, rikkumiste eskaleerimise, erandite käsitlemise ja välise teavitamise eest.

3.5 Tagada organisatsiooni õigusliku ja regulatiivse vastavuse auditeeritavus ning põhjendatavus kontrollide, uurimiste või sertifitseerimise hindamiste käigus.

4. Rollid ja vastutused

4.1 Tippjuhtkond

4.1.1 Vastutab strateegilisel tasandil organisatsiooniülese õigusliku ja regulatiivse vastavuse eest.

4.1.2 Vaatab läbi ja kiidab heaks kõrge riskiga vastavusotsused, sealhulgas riskide aktsepteerimise ja õigusvaidlused.

4.2 Vastavusjuht / peajurist / õigusnõustaja

4.2.1 Hoiab käigus vastavuskohustuste registrit, milles on loetletud kõik kohaldatavad seadused, standardid, sertifikaadid ja lepingutingimused.

4.2.2 Viib läbi uute teenuste, turgude või andmevoogude õigusmõju hindamisi.

4.2.3 Annab organisatsiooni jaoks siduva tõlgenduse seaduste ja standardite kohaldamise kohta.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Iga-aastane poliitika läbivaatamine

9.1.1 Käesolev poliitika tuleb läbi vaadata vähemalt üks kord kalendriaastas, et:

9.1.1.1 tagada jätkuv kooskõla ajakohastatud õigusnormide, valdkonna standardite ja regulatiivsete raamistikega;

9.1.1.2 valideerida tegevuslik tõhusus auditileidude ja intsidentide ajaloo põhjal;

9.1.1.3 kajastada organisatsioonilisi muudatusi (nt uued jurisdiktsioonid, süsteemid või ärisuunad).

9.2 Sündmuspõhised läbivaatamised

9.2.1 Vahepealsed läbivaatamised tuleb algatada, kui:

9.2.2 jõustub või ajakohastatakse uus õiguslik või regulatiivne nõue;

9.2.3 vastavusintsident või audit toob esile poliitika puudused;

9.2.4 organisatsioon siseneb uuele turule või teenusvaldkonda, millele kohaldub eraldiseisev vastavusraamistik;

9.2.5 järelevalvepraktika suundumused või regulaatori juhised viitavad muutustele riskipositsioonis.

9.3 Omanik ja heakskiit

9.3.1 Õigusosakond ja vastavusjuht vastutavad ühiselt läbivaatamisprotsessi koordineerimise eest.

9.3.2 Poliitika lõplikud muudatused peab heaks kiitma tippjuhtkond ning need tuleb kanda poliitikamuudatuste registrisse koos seotud muudatuste juhtimise viidete ja teavitusplaanidega.

9.4 Versioonihaldus ja teavitamine

9.4.1 Käesoleva poliitika iga ajakohastatud versioon peab:

9.4.1.1 sisaldama peamiste muudatuste kokkuvõtet;

9.4.1.2 olema ametlike kanalite kaudu uuesti edastatud (nt poliitikaportaal, LMS, siseuudiskirjad);

9.4.1.3 nõudma kinnitust mõjutatud töötajatelt, eelkõige õigus-, tegevus-, turbe- ja tarnijahalduse rollides töötavatelt isikutelt.

10. Seotud poliitikad ja seosed

10.1 Käesolev poliitika toimib koostoimes järgmiste organisatsiooni ISMSi poliitikatega ja tugevdab neid:

10.1.1 P1 – Infoturbepoliitika: kehtestab juhtimise aluspõhimõtted, mis tagavad, et kõik infoturbepoliitikad, sealhulgas vastavusega seotud poliitikad, on kooskõlas strateegiliste äri- ja regulatiivsete nõuetega.

10.1.2 P2 – Juhtimisrollide ja vastutuste poliitika: määratleb otsustusõigused, sealhulgas õigus- ja vastavusrollid, mis vastutavad regulatiivse järelevalve ja aruandekohustuse eest.

10.1.3 P6 – Riskijuhtimise poliitika: toetab õigusliku ja regulatiivse vastavusega seotud riskide hindamist, riskivastutust ja maandamist kogu organisatsioonis.

10.1.4 P8 – Infoturbeteadlikkuse koolituse poliitika: tagab, et kõik töötajad on teadlikud vastavuskohustustest ja saavad oma rollile vastavat koolitust.

10.1.5 P12 – Varahalduse poliitika: tugevdab õiguslikke kohustusi reguleeritud või lepinguliste varade haldamisel ja kaitsmisel, sealhulgas isikuandmeid ja kriitilist taristut hõlmavate varade puhul.

10.1.6 P30 – Intsidentidele reageerimise poliitika: reguleerib kohustuslikke õiguslikke teavitusi (nt GDPR artikkel 33) ja eskaleerimisprotseduure vastavusrikkumise või regulatiivse sündmuse korral.

10.1.7 P33 – Auditi ja vastavusseire poliitika: sätestab struktureeritud kindlustandvad tegevused, sealhulgas kontrollimeetmete testimise ja tõendusmaterjali kogumise, mis on vajalikud sisemiseks ja väliseks vastavuse kontrollimiseks.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 4.2 – Huvitatud osapoolte vajaduste ja ootuste mõistmine: nõuab õiguslike ja regulatiivsete nõuete tuvastamist ning lõimimist ISMSi.

11.1.2 Punkt 5.1 – Eestvedamine ja pühendumus: nõuab tippjuhtkonna vastutust õigusnormidele vastavuse kehtestamise ja hoidmise eest organisatsioonis.

11.1.3 Punkt 5.3 – Organisatsioonilised rollid, vastutused ja volitused: tagab õigusliku järelevalve ja regulatiivse vastavusega seotud rollide selguse.

11.1.4 Lisa A kontrollimeede 5.36 – Vastavus õiguslikele ja lepingulistele nõuetele: kehtestab seadustest, õigusnormidest ja lepingutest tulenevate kohustuste tuvastamise ja täitmise nõude.

11.2 ISO/IEC 27002

11.2.1 Kontrollimeede 5.36: kirjeldab rakendusjuhiseid vastavuskohustuste registri pidamiseks, regulatiivsete nõuete valideerimiseks ja struktureeritud tõendusmaterjali säilitamise tagamiseks.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Turbe planeerimise poliitika ja protseduurid: nõuab, et vastavusnõuded oleksid lõimitud juhtimisstruktuuridesse ja dokumentatsiooni.

11.3.2 PM-1 – Infoturbeprogrammi plaan: nõuab regulatiivsete kontrollimeetmete käsitlemist laiema turbeprogrammi osana.

11.3.3 CA-7 – Pidev seire: toetab kontrollimeetmete tõhususe järelevalvet õiguslike ja poliitikanõuete täitmisel.

11.3.4 AU-9 – Auditiinfo kaitse: tagab, et vastavusega seotud auditilogid ja kirjed on kaitstud ning kontrollimiseks kättesaadavad.

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

11.4.1 Artikkel 5 – Isikuandmete töötlemise põhimõtted: nõuab õiguspärast töötlemist, läbipaistvust ja vastutust.

11.4.2 Artikkel 6 – Töötlemise õiguspärasus: nõuab kõigile andmetöötlustoimingutele asjakohast õiguslikku alust.

11.4.3 Artikkel 24 – Vastutava töötleja kohustused: kehtestab otsese vastutuse regulatiivse vastavuse tagamise eest.

11.4.4 Artikkel 32 – Töötlemise turvalisus: nõuab asjakohaste tehniliste ja korralduslike meetmete rakendamist.

11.4.5 Artikkel 33 – Isikuandmete rikkumisest teatamine: nõuab isikuandmete rikkumisest teatamist pädevale järelevalveasutusele 72 tunni jooksul.

11.5 ELi NIS2 direktiiv (2022/2555)

11.5.1 Artiklid 20–21: nõuavad, et olulised ja tähtsad üksused rakendaksid dokumenteeritud juhtimist, õigusnormidele vastavuse strateegiaid ja õiguslike riskide pidevat läbivaatamist.

11.6 ELi DORA (2022/2554)

11.6.1 Artikkel 5(2) – IKT-riski juhtimise raamistik: nõuab õigusnormidele vastavuse lõimimist laiematesse riskijuhtimise ja järelevalve funktsioonidesse.

11.6.2 Artikkel 19 – IKT kolmanda isiku risk: kehtestab konkreetsed õiguslikud nõuded lepinguliste ja regulatiivsete kohustuste haldamiseks, mis on seotud väliste tarnijate ja platvormidega.

11.7 COBIT 2019

11.7.1 APO12 – Riski juhtimine: käsitleb õiguslikku ja regulatiivset vastavust organisatsiooni riskijuhtimise kriitilise osana.

11.7.2 MEA03 – Vastavuse seire väliste nõuete suhtes: määratleb pideva seire, erandite käsitlemise ja auditivalmiduse kõigi regulatiivsete kohustuste vormide puhul.