					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P12					Dokumendi pealkiri: **Varahalduse 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 kohustuslikud organisatsioonilised nõuded teabevarade tuvastamiseks, klassifitseerimiseks, haldamiseks ja kaitsmiseks kogu nende elutsükli vältel. See toetab riistvara-, tarkvara-, andme-, pilve- ja immateriaalsete teabevarade organisatsiooniülest juhtimist, sealhulgas mobiilsetes, kaugtöö- ja kolmandate osapoolte hallatavates keskkondades.

1.2 Käesoleva poliitika eesmärk on tagada täielik nähtavus organisatsiooni teabevarade maastikust, et võimaldada tõhusate turbekontrollide rakendamist, omanike määramist, vastavusnõuete täitmise tagamist ning vastutustundlikku kasutuselt kõrvaldamist või hävitamist.

1.3 Käesolev poliitika on kooskõlas standardi ISO/IEC 27001:2022 lisa A kontrollmeetmega A.5.9, nõudes teabe ja sellega seotud varade tsentraliseeritud registri pidamist. See tagab vastutuse, sidudes iga vara omanikuga, ning rakendades klassifikatsioonipõhist kaitset vastavalt ärilisele tundlikkusele ja regulatiivsetele nõuetele.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib kõigile töötajatele, töövõtjatele, kolmandatest osapooltest tarnijatele ja teenuseosutajatele, kes haldavad, kasutavad, võimaldavad juurdepääsu, säilitavad või töötlevad organisatsiooni omandis või kontrolli all olevaid teabevarasid.

2.2 Kohaldamisala hõlmab kõiki varakategooriaid, sealhulgas:

2.2.1 Füüsilised varad: sülearvutid, lauaarvutid, mobiilseadmed, eemaldatavad andmekandjad, printerid, võrguseadmed

2.2.2 Digitaalsed varad: tarkvara, rakendused, süsteemitõmmised, andmebaasid, varukoopiad, krüptovõtmed

2.2.3 Teabevarad: struktureeritud ja struktureerimata andmed, aruanded, e-kirjad, intellektuaalomand

2.2.4 Pilve- ja virtuaalvarad: IaaS-, SaaS- ja PaaS-keskkonnad, virtuaalmasinad, konteinerid

2.2.5 Loogilised varad: domeeninimed, litsentsid, kasutajakontod, lähteseadistused

2.3 Käesolev poliitika reguleerib ka kaugtöö-, hübriid- või allhankekeskkonnas kasutatavaid varasid, tagades nende kaitse ja nähtavuse ka juhul, kui varad ei asu füüsiliselt organisatsiooni ruumides.

3. Eesmärgid

3.1 Hoida kõigi organisatsiooni teabevarade kohta täielikku, täpset ja ajakohast vararegistrit, milles on määratud omanik, klassifikatsioon ja asukohateave.

3.2 Määrata varaomanikud, kes vastutavad nende kontrolli all olevate varade klassifitseerimise, käitlemise ja kaitse eest kooskõlas andmehalduse ja infoturbe poliitikatega.

3.3 Rakendada kõigile varadele asjakohane klassifitseerimine ja märgistamine lähtuvalt tundlikkusest, kriitilisusest ja regulatiivsetest kaalutlustest.

3.4 Kaitsta varasid vastavalt nende klassifikatsioonile ja seotud riskitasemele, sealhulgas säilitamise, juurdepääsu, edastamise ja kõrvaldamise osas.

3.5 Tagada vara tagastamise ja turvalise kasutuselt kõrvaldamise protseduuride rakendamine töötaja lahkumise, lepingu lõpetamise või vara elutsükli lõppemise korral.

3.6 Toetada vastavust sellistele raamistikele nagu ISO/IEC 27001, GDPR, NIS2, DORA ja COBIT 2019 struktureeritud varahalduse ning auditeeritavuse kaudu.

4. Rollid ja vastutused

4.1 Tippjuhtkond

4.1.1 Kinnitab varahalduse poliitika ja tagab selle täielikuks rakendamiseks vajalike ressursside eraldamise.

4.1.2 Kannab lõppvastutust selle eest, et organisatsiooni varad oleksid kaitstud ja hallatud kooskõlas regulatiivsete ja lepinguliste kohustustega.

4.2 Infoturbe juht

4.2.1 Vastutab varahalduse poliitika eest ning tagab selle lõimimise organisatsiooni infoturbe juhtimissüsteemiga (ISMS).

4.2.2 Vaatab läbi käesoleva poliitika erandid ja kõrvalekalded ning rakendab riskipõhiseid maandamismeetmeid.

4.2.3 Teostab järelevalvet perioodiliste auditite üle, mis käsitlevad vara klassifitseerimist, registri terviklikkust ja vara elutsükli vastavust.

[... 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 vastusena järgmisele:

9.1.1 Õiguslike või regulatiivsete kohustuste muudatused, mis mõjutavad vara klassifitseerimist või registri pidamise nõudeid

9.1.2 Uute varakategooriate või haldusplatvormide kasutuselevõtt (nt pilvepõhised CMDB-d)

9.1.3 Siseauditi leiud või turbeintsidendid, mis on seotud varade väärhaldusega

9.1.4 Organisatsioonilised ümberkorraldused, mis mõjutavad omandit või elutsükli kontrollimeetmeid

9.2 Läbivaatamisprotsessi algatab IT varahaldur ning seda koordineeritakse infoturbe juhi, hanke, õigusfunktsiooni ja asjaomaste osakonnajuhtidega.

9.3 Vahepealsed läbivaatused võivad käivituda ka järgmistel alustel:

9.3.1 Äriüksuste omandamine või võõrandamine

9.3.2 Tarnijamuudatused, mis mõjutavad kolmandate osapoolte hallatavaid varasid

9.3.3 Tehnoloogiauuendused, mis hõlmavad massilist kasutuselt kõrvaldamist või provisioneerimist

9.4 Kõik käesoleva poliitika muudatused peavad:

9.4.1 Olema versioonihalduse all ja salvestatud ISMS-i hoidlas

9.4.2 Olema kinnitatud tippjuhtkonna poolt

9.4.3 Sisaldama muudatuste kokkuvõtet ja põhjendust

9.4.4 Olema edastatud kõigile asjaomastele sidusrühmadele, sealhulgas ajakohastatud protseduurid või süsteemikoolitused, kui see on asjakohane

10. Seotud poliitikad ja seosed

10.1 Käesolevat poliitikat kohaldatakse koos järgmiste seotud poliitikatega ning see toetab nende rakendamist:

10.1.1 P4 - Juurdepääsukontrolli poliitika: tagab, et varade nähtavus on kooskõlas juurdepääsuõiguste ja kontrollimehhanismidega süsteemides ning andmekeskkondades.

10.1.2 P7 - Töölevõtu ja töösuhte lõpetamise poliitika: reguleerib füüsiliste ja loogiliste varade õigeaegset väljastamist ning tagastamist töötajate liikumise korral.

10.1.3 P13 - Andmete klassifitseerimise ja märgistamise poliitika: kehtestab varade kohustuslikud klassifitseerimisreeglid, millest sõltuvad märgistamise, käitlemise ja kõrvaldamise protseduurid.

10.1.4 P14 - Andmete säilitamise ja kõrvaldamise poliitika: määratleb digitaalseid ja füüsilisi teavet sisaldavaid varasid puudutavad turvalise kõrvaldamise tähtajad ja meetodid.

10.1.5 P22 - Logimis- ja seirepoliitika: võimaldab vara juurdepääsu ja kasutuse jälgitavust süsteemilogide, lõppseadmete nähtavuse ja käitumusliku analüütika kaudu.

10.1.6 P30 - Intsidentidele reageerimise poliitika: toetab varadega seotud rikkumiste, näiteks kadunud sülearvutite või jälgimata salvestuskandjate, kiiret ohjeldamist ja uurimist.

10.2 Need poliitikad moodustavad ühtse juhtimisstruktuuri, mis tagab varade turvalise haldamise, täpse registreerimise ja asjakohase käitlemise kogu nende elutsükli jooksul.

11. Viitestandardid ja raamistikud

11.1 Käesolev poliitika on kooskõlas rahvusvaheliselt tunnustatud infoturbe standardite ja regulatiivsete raamistikega, mis nõuavad tugevat varahaldust kogu elutsükli vältel.

11.2 ISO/IEC 27001:

11.2.1 Punkt 8.1 - nõuab, et organisatsioonid kavandaksid, rakendaksid ja kontrolliksid protsesse, mis on vajalikud infoturbe nõuete täitmiseks, sealhulgas vara elutsükli haldamiseks.

11.3 ISO/IEC 27002:2022 - Kontrollimeetmed 5.9 kuni 5.11

11.3.1 Punkt 5.9 - teabe ja muude seotud varade register: nõuab ajakohast ja täielikku registrit kõigist teabetöötluse seisukohalt asjakohastest varadest.

11.3.2 Punkt 5.10 - teabe ja varade lubatud kasutamine: toetatud kasutusreeglite, omandimudeli ja tagastusprotsessidega.

11.3.3 Punkt 5.11 - varade tagastamine: rakendatud ametlike üleandmise ja kasutuselt kõrvaldamise protseduuride kaudu.

11.3.4 Need kontrollimeetmed kehtestavad struktureeritud nõuded organisatsiooni varade tuvastamiseks, märgistamiseks, haldamiseks ja jälgimiseks ning määravad vastavad kohustused omanikele ja vastutavatele halduritele kogu elutsükli vältel.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CM-8 - süsteemikomponentide register: kajastub tsentraliseeritud varahalduses, reaalajas nähtavuses ja seostes operatiivsete konfiguratsioonidega.

11.4.2 RA-3 - riskihindamine: vararegistrid on ohumudeldamise ja riskihindamise aluskomponendid.

11.4.3 MP-6 - andmekandjate puhastamine: rakendatakse vara elutsükli kontrollimeetmetes ja andmete kõrvaldamise poliitikas määratletud turvaliste kõrvaldamismeetodite kaudu.

11.5 EU GDPR (2016/679):

11.5.1 Artikkel 30 - töötlemistoimingute registrid: nõuab, et organisatsioonid dokumenteeriksid süsteemid, seadmed ja hoidlad, mis säilitavad või töötlevad isikuandmeid.

11.5.2 Artikkel 32 - töötlemise turvalisus: on kooskõlas varapõhise riskihindamise ja klassifitseeritud varadele ning kriitilisele taristule kohandatud kaitsemeetmetega.

11.6 EU NIS2 direktiiv (2022/2555):

11.6.1 Artikkel 21(2)(a, b): nõuab vara nähtavust ja registri pidamist kui riskianalüüsi, kaitse ja küberturbeintsidentidele reageerimise alust.

11.6.2 Artikkel 21(3): rõhutab struktureeritud varahalduse vajalikkust organisatsiooni turbeteadliku kultuuri osana.

11.7 EU DORA (2022/2554):

11.7.1 Artikkel 5 - IKT juhtimine ja sisekontroll: nõuab, et finantsüksused kontrolliksid IKT-varasid selge registri, omandimudeli ja kaitsenõuetega.

11.7.2 Artikkel 9 - IKT-riskide juhtimise raamistik: sätestab, et varahalduse protsessid peavad toetama ohtude maandamist, talitluspidevuse planeerimist ja teenuste toimepidevust.

11.8 COBIT 2019:

11.8.1 BAI09 - varade haldamine: on otseselt kooskõlas organisatsiooni varade struktureeritud tuvastamise, klassifitseerimise, kasutamise ja kõrvaldamisega.

11.8.2 DSS01 - hallatud operatsioonid: toetab selliste kontrollimeetmete rakendamist, mis tagavad vara kaitse ja operatiivjuhtimise järjepidevuse.

11.8.3 MEA03 - vastavuse seire, hindamine ja auditeerimine: tagab varahalduse kontrollimeetmete ja nende tõhususe regulatiivse kooskõla seisukohalt korrapärase auditeerimise.