					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P14					Dokumendi pealkiri: **Andmete säilitamise ja kõrvaldamise 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/õigusnorm	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punktid 6.1.3, 8.1	
ISO/IEC 27002:2022	Kontrollimeetmed 5.10, 5.12, 5.30, 5	
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12, PL-2	
ELi GDPR	Artiklid 5(1)(e), 17, 32	
ELi NIS2	Artikkel 21(2)(a-e)	
ELi DORA	Artiklid 5, 9	
COBIT 2019	DSS01, DSS05, MEA	

1. Eesmärk

1.1 Käesoleva poliitika eesmärk on kehtestada organisatsioonilised nõuded andmete säilitamiseks ja turvaliseks kõrvaldamiseks kogu teabe elutsükli vältel. See tagab vastavuse kohaldatavatele õiguslikele, regulatiivsetele ja lepingulistele kohustustele ning hoiab ära andmete tarbetu või riskantse kuhjumise.

1.2 Käesolev poliitika toetab standardi ISO/IEC 27001:2022 rakendamist, kehtestades kontrollimeetmed andmete säilitustähtaegade ja pöördumatute kõrvaldamistavade üle. See võimaldab pidada jälgitavat dokumentatsiooni kirjete kohta, rakendada teabe klassifikatsiooni tundlikkusega kooskõlas olevat säilitamist ning tagada suutlikkuse tõendada vastavust auditi, regulatiivse järelevalve ja õigusliku tõendamise korral.

1.3 Lisaks on poliitika eesmärk tagada andmete konfidentsiaalsus, terviklus ja käideldavus, vähendades samal ajal äririski, tegevuslikku ebatõhusust ja andmekaitserikkumistega seotud riskipositsiooni, mis võib tuleneda andmete valest säilitamisest või hävitamisest.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub kõigile füüsilistele ja digitaalsetele teabevaradele, mis kuuluvad organisatsioonile või mida organisatsioon töötleb või säilitab, sealhulgas varadele, mis on kolmandate isikute, tütarettevõtjate või allhankepartnerite kontrolli all.

2.2 Kohaldamisala hõlmab muu hulgas järgmist:

2.2.1 dokumendid, failid ja kirjed (digitaalsel ja paberkandjal)

2.2.2 andmebaasid ja arhiivid

2.2.3 e-kirjad ja kiirsuhtluse logid

2.2.4 varukoopiad, süsteemilogid ja auditijäljed

2.2.5 lähtekood, rakenduste andmed ja pilvekeskkonnas majutatud varad

2.2.6 eemaldatavad andmekandjad ja kasutuselt kõrvaldatud riistvara, mis sisaldab andmeid

2.3 Poliitika reguleerib nii tegevuskirjeid kui ka reguleeritud andmekogumeid (nt finants-, õigus-, personali-, kliendi- ja auditiga seotud sisu) sõltumata säilituskohast või süsteemist.

2.4 See kohaldub kõigile organisatsiooni üksustele ning kõigile töötajatele, töövõtjatele ja tarnijatele, kes osalevad andmete loomises, säilitamises, haldamises või kõrvaldamises.

3. Eesmärgid

3.1 Tagada, et andmeid säilitatakse ainult seni, kuni see on õiguslikult, lepinguliselt või tegevuslikult vajalik, ning et need kõrvaldatakse turvaliselt, kui neid enam ei vajata.

3.2 Vältida kirjete enneaegset, loata või juhuslikku kustutamist, kui neid on vaja käimasoleva tegevuse, vastavuse, kohtuvaidluse või auditi eesmärgil.

3.3 Kehtestada ja rakendada järjepidevad säilitustähtajad, mis põhinevad andmete klassifikatsioonil, vara tüübil, kohaldatavatel õigusnormidel ja riskipositsioonil.

3.4 Kaitsta andmete privaatsust ja konfidentsiaalsust säilitamisperioodi jooksul ning kõrvaldamise hetkel, sealhulgas andmesubjekti õiguste täitmisel (nt kustutamine GDPR artikli 17 alusel).

3.5 Tagada, et kõik andmete kõrvaldamise meetodid on pöördumatud, asjakohaselt dokumenteeritud ja kooskõlas tunnustatud standarditega, nagu NIST SP 800-88.

3.6 Vähendada tegevuslikku ebatõhusust, kulukoormust ja õiguslikku riskipositsiooni, mis tuleneb ülemäärasest säilitamisest või jälgimata pärandandmetest.

3.7 Toetada talitluspidevuse ja katastroofitaaste eesmärke integreeritud varukoopiate säilitamise halduse ja põhjendatud andmearhiveerimise tavade kaudu.

4. Rollid ja vastutusalad

4.1 Tippjuhtkond

4.1.1 kiidab käesoleva poliitika heaks ning tagab asjakohase rahastuse, ressursside olemasolu ja lõimimise ettevõtte riskijuhtimise ning vastavusprogrammidega.

4.1.2 vastutab üldiselt andmete säilitamise ja turvalise kõrvaldamisega seotud õiguslikele ja regulatiivsetele nõuetele vastavuse eest.

4.2 Infoturbe juht

4.2.1 on käesoleva poliitika omanik ning vastutab säilitamise ja kõrvaldamise halduse määratlemise ja läbivaatamise eest kooskõlas ISMS-iga.

4.2.2 tagab, et klassifikatsioonil põhinevad säilitamise ja kõrvaldamise nõuded rakendatakse äriüksustes ja tehnilistes süsteemides.

4.2.3 teostab vastavuse seiret ning rakendab vajaduse korral parandusmeetmeid.

[... 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 kord aastas või siis, kui esineb üks järgmistest tingimustest:

9.1.1 muudatused kohaldatavates õigusaktides või regulatsioonides, mis mõjutavad andmete säilitamist (nt GDPR-i, maksueeskirjade või DORA ajakohastused)

9.1.2 muudatused klassifitseerimisraamistikus või äriprotsessides, mis mõjutavad andmete elutsükli etappe

9.1.3 uute IT-süsteemide, arhiveerimisplatvormide või andmekandjate kõrvaldamise tehnoloogiate kasutuselevõtt

9.1.4 siseauditi leiud või regulatiivsed soovitused, mis toovad esile puudujääke säilitamis- või kõrvaldamistavades

9.2 Läbivaatamist juhivad infoturbe juht ja andmekaitseametnik, kaasates õigusfunktsiooni, vastavusfunktsiooni, IT ja äriüksused.

9.3 Andmete säilitamise põhiplaan (MDRS) ja kõrvaldamisregister tuleb läbi vaadata paralleelselt, et tagada:

9.3.1 tähtajad on jätkuvalt täpsed ning kajastavad tegevuslikke, õiguslikke ja regulatiivseid vajadusi

9.3.2 kõrvaldamise dokumentatsioon on täielik ja auditikõlblik

9.3.3 õigusliku säilitamiskohustuse kirjed on valideeritud ja vabastatud, kui see on asjakohane

9.4 Kõik poliitikamuudatused peavad:

9.4.1 olema ametlikult versioonihaldatud ja säilitatud ISMS-i dokumendihoidlas

9.4.2 sisaldama versiooniajalugu ja muudatuse põhjendust

9.4.3 olema tippjuhtkonna poolt heaks kiidetud

9.4.4 olema asjakohastele töötajatele edastatud koos ajakohastatud koolitus- või juhendmaterjalidega

9.5 Oluliste poliitikamuudatuste korral peavad mõjutatud töötajad jätkuva vastavuse tagamiseks läbima sihipärase koolituse 30 päeva jooksul alates muudatuse avaldamisest.

9.6 Seotud poliitikad ja seosed

10. Seotud poliitikad ja seosed

10.1.1 P4 - Juurdepääsukontrolli poliitika: tagab, et andmetele pääsevad säilitamisperioodi jooksul juurde ainult volitatud isikud ning et aegunud andmed on kuni kõrvaldamiseni piiratud.

10.1.2 P12 - Varahalduse poliitika: määrab kindlaks, millised varad sisaldavad ajastatud kõrvaldamist vajavaid andmeid, ning jälgib nende elutsüklit alates soetamisest kuni hävitamiseni.

10.1.3 P13 - Andmete klassifitseerimise ja märgistamise poliitika: suunab klassifitseerimisotsuseid, mis mõjutavad otseselt andmete säilitamise kestust ja nõutavat kõrvaldamismeetodit.

10.1.4 P15 - Varundamise ja taastamise poliitika: määrab varukoopiate andmekandjate ja replikeeritud andmevarade säilitustähtajad ning kõrvaldamisprotseduurid.

10.1.5 P18 - Krüptograafiliste kontrollimeetmete poliitika: toetab krüptograafilist pühkimist kõrvaldamise eesmärgil ning nõuab andmete krüpteerimist säilitamise ajal kuni hävitamiseni.

10.1.6 P30 - Intsidentidele reageerimise poliitika: rakendub juhtudel, kui ebaõige kõrvaldamine põhjustab võimalikku andmekadu, andmekaitserikkumist või regulatiivset rikkumist.

10.2 Igal seotud poliitikal on roll ühtse andmehaldusmudeli rakendamisel klassifitseerimise, elutsükli kontrolli, juurdepääsu ja auditivalmiduse lõikes.

11. Viitestandardid ja raamistikud

11.1 Käesolev poliitika on kooskõlas rahvusvaheliselt tunnustatud standardite ja regulatiivsete raamistikega, mis määratlevad turvalised, nõuetele vastavad ja tõhusad andmete elutsükli tavad.

11.2 ISO/IEC 27001:

11.2.1 punkt 6.1.3 - riski käsitlemise plaan: toetab ülemäärase säilitamise, andmekaitserikkumiste või kõrvaldamise tõrgetega seotud riskide maandamist.

11.2.2 punkt 8.1 - tegevuste kavandamine ja ohje: kehtestab elutsükli kontrollimeetmed, mis reguleerivad säilitamist, arhiveerimist ja hävitamist.

11.3 ISO/IEC 27002:2022 - kontrollimeetmed 5.10, 5.12, 5.30, 5: annavad praktilised suunised andmete lubatud kasutuse, säilitamise põhjendatuse, kontrollitud kustutamise ja põhjendatud kirjete halduse kohta kooskõlas organisatsiooni riskitaluvusega.

11.4 NIST SP 800-53 Rev. 5:

11.4.1 AU-11 - auditikirjete säilitamine: tagab auditilogide ja vastavuse tõendusmaterjali piisava säilitamise.

11.4.2 MP-6 - andmekandjate puhastamine: nõuab füüsiliste ja elektrooniliste andmekandjate turvalisi, dokumenteeritud hävitamismeetodeid.

11.4.3 SI-12 - teabe käitlemine: rakendab asjakohast andmekäsitlust kooskõlas säilitamise ja kõrvaldamise kontrollimeetmetega.

11.4.4 PL-2 - süsteemi turbe- ja andmekaitseplaan: nõuab süsteemipõhist dokumentatsiooni andmete elutsükli käitlemise ja turvalise kõrvaldamise nõuete kohta.

11.5 ELi GDPR (2016/679):

11.5.1 artikkel 5(1)(e) - andmete minimeerimine ja säilitamise piirang: nõuab, et andmeid ei säilitataks kauem kui vajalik.

11.5.2 artikkel 17 - õigus andmete kustutamisele („õigus olla unustatud“): nõuab isikuandmete kiiret ja püsivat kustutamist põhjendatud taotluse korral.

11.5.3 artikkel 32 - töötlemise turvalisus: tugevdab andmekaitset säilitamise ajal ja nõuab aegunud kirjete turvalist hävitamist.

11.6 ELi NIS2 direktiiv (2022/2555):

11.6.1 artikkel 21(2)(a-e): nõuab, et üksused võtaksid kasutusele poliitikad ja tehnilised meetmed andmete turvaliseks käitlemiseks, sealhulgas säilitamise piirangud ja kõrvaldamismeetodid.

11.7 ELi DORA (2022/2554):

11.7.1 artikkel 5 - juhtimine ja kontroll: nõuab struktureeritud IKT-riskijuhtimist, sealhulgas teabe elutsükli turvalist haldamist.

11.7.2 artikkel 9 - IKT-riskijuhtimise raamistik: nõuab poliitikaid andmete säilitamise, hävitamise ning digitaalsete tegevuste õigusliku ja regulatiivse vastavuse kohta.

11.8 COBIT 2019:

11.8.1 DSS01 - hallatud operatsioonid: toetab säilitamise jälgimist ja järjepidevust andmesüsteemides.

11.8.2 DSS05 - hallatud turbeteenused: tagab säilitatud ja arhiveeritud andmete kaitse kuni nende turvalise kõrvaldamiseni.

11.8.3 MEA03 - vastavuse seire, hindamine ja auditeerimine: võimaldab auditeerida säilitamise rakendamist, kustutamisprotseduure ja regulatiivsete nõuete täitmist.