					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P14S					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 õigusaktidega

Standard/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punktid 6.1.3, 8	Hõlmab riskikäsitlust, operatiivseid kontrollimeetmeid ja säilitamisnõudeid
ISO/IEC 27002:2022	Kontroll 5	Suunised säilitustähtaegade ja turvaliste hävitusmeetodite määramiseks
NIST SP 800-53 Rev.5	AU-11, MP-6, SI-12	Auditikirjete säilitamine, andmekandjate puhastamine, andmete säilitamise piirangud ja nende rakendamine
EL NIS2	Artikkel 21(2)(a)	Nõutav on riskikohane elutsükli halduse poliitika
EL DORA	Artikkel 5(1)	IKT-riskide juhtimine: andmete käideldavus ja eemaldamine
COBIT 2019	BAI03.04, DSS01	Teabe elutsükli kontrollimeetmed, turvaline kõrvaldamine
EL isikuandmete kaitse üldmäärus (GDPR)	Artikkel 5(1)(e), 17	Andmeid ei tohi säilitada kauem kui vajalik; õigus kustutamisele

1. Eesmärk

1.1 Käesoleva poliitika eesmärk on kehtestada VKE keskkonnas rakendatavad nõuded teabe säilitamiseks ja turvaliseks kõrvaldamiseks. Sellega tagatakse, et kirjeid säilitatakse ainult seadusest, lepingulisest kohustusest või ärivajadusest tuleneva aja jooksul ning seejärel hävitatakse need turvaliselt.

1.2 Käesoleva poliitika eesmärk on vähendada teaberiski, hallata õigusriski ja piirata dubleeriva või aegunud teabe säilitamist. See aitab tagada vastavuse standardile ISO/IEC 27001 ja andmekaitseraamistikele, nagu GDPR, minimeerides isikuandmete või tundliku teabe loata säilitamise.

1.3 Hästi struktureeritud säilitamise ja kõrvaldamise raamistik vähendab tegevuskulusid, parandab süsteemide jõudlust ja suurendab auditivalmidust. Piiratud IT-võimekusega VKE-de jaoks pakub see praktilise viisi digitaalsete ja füüsiliste teabevarade vastutustundlikuks haldamiseks.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub järgmisele:

2.1.1 kõik kirjed, failid, logid, teabevahetus ja andmekogumid, mida organisatsioon loob, kogub, töötleb või säilitab;

2.1.2 kõik töötajad, töövõtjad ja välised teenuseosutajad, kes käitlevad organisatsiooni andmeid;

2.1.3 kõik andmevormingud (nt paber, elektrooniline, pilt, heli või logi) ja kõik andmekandjad (nt kohalikud kettad, pilveteenused, e-posti serverid, varukoopiad).

2.2 Kohaldamisala hõlmab järgmist:

2.2.1 äridokumendid (nt arved, lepingud, projektiraportid);

2.2.2 tegevuskirjed (nt logid, juurdepääsuajalugu, varukoopiate hetktõmmised);

2.2.3 isikuandmed (nt personalifailid, kliendisuhtlus, kasutajatoe kirjed);

2.2.4 andmed, mida majutatakse organisatsiooni sees, väliselt või hübriidsüsteemides;

2.2.5 arhiveeritud andmed ja varukoopiad sõltumata sellest, kas need on aktiivsed või kasutuseta.

2.3 Kohaldamisala hõlmab andmete elutsükli kõiki etappe alates loomisest kuni lubatud kõrvaldamiseni.

3. Eesmärgid

3.1 Määratleda ühtsed säilitamisreeglid õiguslike, operatiivsete ja regulatiivsete kriteeriumide alusel.

3.2 Vältida kriitiliste kirjete enneaegset kustutamist ja kõrvaldada ebavajalik andmete kuhjumine.

3.3 Tagada andmete turvaline ja pöördumatu kõrvaldamine, kui säilitamine ei ole enam vajalik.

3.4 Määrata vastutus säilitamis- ja kustutamisotsuste rakendamise eest VKE tasemel, arvestades personaliressursside piiranguid.

3.5 Tagada auditiks sobiv tõendusmaterjal, et näidata nõuetekohast hoolsust standardite ISO 27001, GDPR, NIS2 ja muude raamistike alusel.

3.6 Edendada andmete turvalist käitlemist kogu elutsükli vältel, tekitamata mittespetsialistidest töötajatele tarbetut tehnilist koormust.

4. Rollid ja vastutused

4.1 tegevjuht

4.1.1 kiidab käesoleva poliitika heaks ja vastutab selle rakendamise eest.

4.1.2 tagab, et säilitamise ja kõrvaldamise protseduurid rakendatakse kooskõlas õiguslike ja äririskidega.

4.1.3 annab vajaduse korral loa eranditeks ja õiguslikuks säilitamiskohustuseks.

4.1.4 algatab poliitika läbivaatamised ning kiidab heaks ajakohastused, mis tulenevad äritegevusest või regulatiivsetest muudatustest.

4.2 määratud andmeomanik

4.2.1 määratakse iga andmekategooria jaoks eraldi (nt finantsandmed, personalikirjed, kliendikirjed).

4.2.2 klassifitseerib kirjed ja määrab poliitikast ning õiguslikest suunistest lähtuva asjakohase säilitustähtaja.

4.2.3 annab loa kustutamiseks, kui säilitamisnõuded on täidetud.

4.2.4 toetab siseauditeid, andes konteksti säilitamisloogika ja kõrvaldamissündmuste kohta.

[... 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 üks kord aastas või järgmiste asjaolude ilmnemisel:

9.1.1 muudatused kohaldatavates õigusnormides (nt andmekaitse, finantsaruandlus);

9.1.2 kasutusele võetakse uued süsteemid või protsessid, mis mõjutavad andmete elutsüklit;

9.1.3 auditileiud või intsidendid, mis toovad esile puudused säilitamistavades.

9.2 Läbivaatamiste käigus tuleb tagada, et säilitamisregister on täielik ja kajastab kõiki peamisi kirjete kategooriaid.

9.3 Poliitika ajakohastused peab heaks kiitma tegevjuht ning neist tuleb teavitada mõjutatud töötajaid. Kõige uuem versioon peab olema kättesaadav ja versioonihallatud.

10. Seotud poliitikad ja seosed

10.1 P2S – Juhtimisrollide ja vastutuste poliitika: määratleb poliitika omandiõiguse ja erandite otsustusõiguse.

10.2 P13S – Andmete klassifitseerimise ja märgistamise poliitika: määrab, kuidas säilitamisreeglid seostuvad andmete klassifitseerimisega.

10.3 P12S – Varahalduse poliitika: reguleerib andmekandjaid, mis sisaldavad säilitamisele või kõrvaldamisele kuuluvaid andmeid.

10.4 P17S – Andmekaitse ja privaatsuse poliitika: tagab andmete minimaalsuse ja toetab GDPRi kohast õiguspärast töötlemist.

10.5 P30S – Intsidendihalduse poliitika: rakendub, kui kõrvaldamise või säilitamise puudused põhjustavad võimaliku andmete avaldumise.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 6.1.3: nõuab teabega seotud riskide, sealhulgas säilitamisriskide käsitlemist.

11.1.2 Punkt 8.1: määratleb elutsüklipõhised operatiivsed kontrollimeetmed.

11.2 ISO/IEC 27002

11.2.1 Kontroll 5.33: suunised säilitustähtaegade ja turvaliste hävitusmeetodite määramiseks.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-11: nõuab auditikirjete säilitamist.

11.3.2 MP-6: määratleb andmekandjate puhastamise protseduurid.

11.3.3 SI-12: käsitleb andmete säilitamise piiranguid ja nende rakendamist.

11.4 EL isikuandmete kaitse üldmäärus (GDPR)

11.4.1 Artikkel 5(1)(e): andmeid ei tohi säilitada kauem kui vajalik.

11.4.2 Artikkel 17: õigus kustutamisele kohaldub siis, kui andmete säilitamiseks puudub enam õiguslik alus.

11.5 EL NIS2

11.5.1 Artikkel 21(2)(a): nõuab riskikohaseid organisatsioonilisi poliitikaid, sealhulgas elutsükli haldust.

11.6 EL DORA

11.6.1 Artikkel 5(1): IKT-riskide juhtimine hõlmab andmete käideldavust ja eemaldamist.

11.7 COBIT 2019

11.7.1 BAI03.04: nõutavad on teabe elutsükli kontrollimeetmed.

11.7.2 DSS01.06: turvalise kõrvaldamise protseduurid teabevarade kaitsmise osana.