					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P18S					Dokumendi pealkiri: **Krüptograafiliste kontrollimeetmete 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	Punkt 8	
ISO/IEC 27002:2022	Kontrollimeetmed 8.24, 8.25	
NIST SP 800-53 Rev.5	SC-12 kuni SC-17	
ELi NIS2 direktiiv	Artiklid 21(2)(d), 21(2)(e)	
ELi DORA määrus	Artiklid 6(2)(d), 9(2)(f)	
COBIT 2019	DSS05.01, APO13	
ELi isikuandmete kaitse üldmäärus (GDPR)	Artiklid 32(1)(a), 34	

1. Eesmärk

1.1 Käesolev poliitika kehtestab kohustuslikud nõuded krüptimise ja krüptograafiliste kontrollimeetmete kasutamiseks, et kaitsta äriandmete ja isikuandmete konfidentsiaalsust, terviklust ja autentsust.

1.2 Sellega tagatakse, et krüptograafilisi vahendeid kasutatakse asjakohaselt süsteemides, seadmetes ja pilveteenustes väikeettevõtte tegevuskeskkonnas.

1.3 Käesolev poliitika toetab otseselt ISO/IEC 27001:2022 sertifitseerimist ning aitab organisatsioonil täita Euroopa Liidu isikuandmete kaitse üldmäärusest (GDPR), ELi NIS2 direktiivist ja digitaalse tegevuskerksuse määrusest (DORA) tulenevaid õiguslikke kohustusi.

1.4 Käesoleva poliitika kohaldamisalasse kuuluvad krüptograafilised kontrollimeetmed hõlmavad andmete krüptimist, sertifikaatide haldust, võtmete turvalist käitlemist ja krüpteeritud varukoopiaid.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib järgmisele:

2.1.1 Kõik töötajad, töövõtjad ja kolmandad isikud, kes käitlevad ettevõtte andmeid

2.1.2 Kõik ärisüsteemid, lõppseadmed ja pilveplatvormid, mida kasutatakse konfidentsiaalse teabe talletamiseks, edastamiseks või sellele juurdepääsuks

2.1.3 Kõik isiku-, finants-, õigus- või muud tundlikud andmed, mis on klassifitseeritud organisatsiooni andmete klassifitseerimise poliitika alusel

2.1.4 Kõik krüptograafilised kontrollimeetmed, sealhulgas krüptimismeetodid, võtmed, paroolid, sertifikaadid ja turvamoodulid

2.2 Poliitika hõlmab andmeid puhkeolekus, andmeid edastamisel ja andmeid kasutamisel. Samuti reguleerib see varukoopiate, e-posti, väliste andmeedastuste ja avalike veebilehtede jaoks kasutatavat krüptimist.

3. Eesmärgid

3.1 Tagada, et tundlikud ja reguleeritud andmed on alati kaitstud asjakohaste krüptograafiliste meetmetega

3.2 Määrata vastutus krüptimisvahendite valiku, seadistuse ja võtmehalduse eest

3.3 Ennetada loata juurdepääsu, turvaintsidente või andmeleket, rakendades turvalise edastamise ja salvestamise kontrollimeetmeid

3.4 Täita õiguslikke ja regulatiivseid nõudeid, mis kohustavad krüptima isikuandmeid ja äriandmeid

3.5 Tagada talitluspidevus ja käideldavus sertifikaatide ja krüptograafiliste võtmete tõhusa halduse kaudu

4. Rollid ja vastutused

4.1 Tegevjuht (GM)

4.1.1 Kinnitab käesoleva poliitika ja tagab krüptograafiliste nõuete rakendamise

4.1.2 Vaatab läbi erandid, rikkumiste teavitused ja tarnijate vastavuse krüptimist käsitlevatele lepingutingimustele

4.1.3 Tagab, et allhanketeenused ja pilveteenused vastavad krüptimisstandarditele

4.2 IT-toe teenuseosutaja / sisemine IT-vastutaja

4.2.1 Rakendab ja haldab krüptimislahendusi (nt täisketta krüptimine, SSL/TLS-sertifikaadid, VPN-id)

4.2.2 Haldab krüptograafiliste võtmete elutsüklit ja turvalisi säilituslahendusi

4.2.3 Seadistab ja seirab varundamise, veebilehtede ja seadmekaitse krüptimist

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Iga-aastane läbivaatamine

9.1.1 Käesolev poliitika tuleb läbi vaadata vähemalt üks kord aastas tegevjuhi poolt koostöös IT-toe teenuseosutaja ja andmekaitsekoordinaatoriga.

9.2 Vahepealse läbivaatamise alused

9.2.1 Läbivaatamine tuleb teha ka juhul, kui:

9.2.1.1 Krüptograafilised standardid või protokollid muutuvad (nt algoritmi kasutuselt kõrvaldamine)

9.2.1.2 Kasutusele võetakse uued süsteemid või pilveteenused

9.2.1.3 Rikkumine või intsident hõlmab kompromiteeritud võtit või sertifikaati

9.2.1.4 Õiguslikud või regulatiivsed muudatused mõjutavad krüptimisnõudeid

9.3 Versioonihaldus ja teabevahetus

9.3.1 Kõik poliitikamuudatused tuleb dokumenteerida versioonihaldusega muudatuste logis

9.3.2 Töötajaid tuleb muudatustest teavitada ning varasemad versioonid arhiveerida

9.3.3 Viimane heaks kiidetud versioon tuleb säilitada poliitikate keskhoidlas

10. Seotud poliitikad ja seosed

10.1 Käesolevat poliitikat tuleb rakendada koos järgmiste VKE poliitikatega:

10.1.1 P12S – Varahalduse poliitika: tagab, et krüptimist rakendatakse klassifitseeritud varadele salvestamisel, edastamisel ja kõrvaldamisel.

10.1.2 P14S – Andmete säilitamise ja kõrvaldamise poliitika: määratleb säilitustähtajad ja nõuab andmete krüpteeritud säilitamist kuni nende turvalise kustutamiseni.

10.1.3 P17S – Andmekaitse ja privaatsuse poliitika: viib krüptimise kooskõlla andmekaitsepõhimõtete ja GDPR artikli 32 regulatiivsete ootustega.

10.1.4 P22S – Logimise ja seire poliitika: nõuab auditieesmärkidel võtmekasutuse, krüptimise tõrgete ja sertifikaatide aegumise logimist.

10.1.5 P30S – Intsidentidele reageerimise poliitika: kirjeldab eskaleerimise, ohjeldamise ja teavitamise protseduure juhtudel, kui krüptimine ebaõnnestub või võtmed kompromiteeritakse.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 8.1 – nõuab turvariskide haldamiseks operatiivsete kontrollimeetmete, sealhulgas krüptimise, rakendamist.

11.2 ISO/IEC 27002

11.2.1 Kontrollimeede 8.24 – kirjeldab nõudeid krüptimise rakendamiseks konfidentsiaalsuse ja tervikluse tagamiseks.

11.2.2 Kontrollimeede 8.25 – käsitleb krüptograafiliste võtmete ja sertifikaatide turvalist haldust.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-12 – kehtestab krüptograafiliste võtmete halduse ja kaitse nõuded.

11.3.2 SC-13 – määratleb krüptograafilise kaitse rakendamise nõuded.

11.3.3 SC-17 – hõlmab avaliku võtme taristut (PKI) ja sertifikaatide elutsükli haldust.

11.3.4 SC-28 – nõuab puhkeolekus andmete krüptimist.

11.3.5 SC-12 kuni SC-17 (perekond) – tagab, et krüptograafilised kaitsemeetmed on süsteemides nõuetekohaselt rakendatud.

11.4 ELi isikuandmete kaitse üldmäärus (GDPR)

11.4.1 Artikkel 32(1)(a) – nõuab, et organisatsioonid rakendaksid andmete konfidentsiaalsuse tagamiseks tehnilisi meetmeid, näiteks krüptimist.

11.4.2 Artikkel 34 – sätestab, et krüptimine võib vabastada organisatsiooni rikkumisest teavitamise kohustusest, kui andmed olid volitamata isikutele arusaamatud.

11.5 ELi NIS2 direktiiv

11.5.1 Artikkel 21(2)(d) – nõuab süsteemide ja side kaitsmiseks tõhusa krüptimise kasutamist.

11.5.2 Artikkel 21(2)(e) – rõhutab andmete kaitset ja küberohtude maandamist krüptimise abil.

11.6 ELi DORA määrus

11.6.1 Artikkel 6(2)(d) – nõuab, et IKT-süsteemides kasutataks turvalisi sidekanaleid ja krüptimist.

11.6.2 Artikkel 9(2)(f) – kohustab finantsüksusi kasutama tugevat krüptimist digitaalsete sidekanalite ja andmevahetuse kaitsmiseks.

11.7 COBIT 2019

11.7.1 DSS05.01 – nõuab tundliku teabe kaitsmist krüptimise ja krüptograafiliste protokollide abil.

11.7.2 APO13.02 – nõuab infoturbe kavandamise osana tõhusate turvakontrollide, sealhulgas krüptograafiliste kaitsemeetmete, rakendamist.