					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: P18					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/õigusnorm	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 8	-
ISO/IEC 27002:2022	Kontrollimeetmed 8.24, 8.25, 8	-
NIST SP 800-53 Rev.5	SC-12 kuni SC-17, SC-28, SC-28(1), SC-12(3)	-
ELi isikuandmete kaitse üldmäärus (GDPR)	Artikkel 32, artiklid 33–34, põhjendus 83	-
ELi NIS2	Artikkel 21(2)(d)	-
ELi DORA	Artiklid 6(2)(d), 11(1)(c)	-
COBIT 2019	DSS05.01, DSS06.06, MEA	-

1. Eesmärk

1.1 Käesolev poliitika sätestab kohustuslikud nõuded krüptograafiliste kontrollimeetmete turvaliseks ja nõuetele vastavaks kasutamiseks kogu organisatsioonis, et tagada tundliku ja reguleeritud teabe konfidentsiaalsus, terviklus ja autentsus.

1.2 Krüptograafia kasutamine on andmeturbe toimingute usaldusväärsuse alus, toetab turvalist teabevahetust, võimaldab rakendada juurdepääsukontrolli ning aitab täita õigus- ja regulatiivseid nõudeid tõhusa krüpteerimise ja võtmehalduse tavade kaudu.

1.3 Käesolev poliitika on kooskõlas standardi ISO/IEC 27001:2022 punktiga 8.1 ja lisa A kontrollimeetme 8.24 nõuetega ning toetab GDPRi artiklist 32, DORA artiklist 6(2)(d) ja NIS2 artiklist 21 tulenevate õiguslike ja tegevuslike kohustuste täitmist. Samuti toetab see COBIT 2019 eesmärke turvateenuste ja andmevarade kaitse valdkonnas.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib kõigi organisatsiooni üksuste, ärifunktsioonide, töötajate ja kolmandatest osapooltest teenuseosutajate suhtes, kes kasutavad, haldavad või rakendavad krüptograafilisi tööriistu ja meetodeid.

2.2 Hõlmatud on tootmis-, arendus-, test-, varundus- ja katastroofitaastesüsteemid, milles tundlikke andmeid edastatakse, töödeldakse või säilitatakse.

2.3 Kohaldamisala hõlmab kõiki krüptograafilisi komponente ja kasutusjuhtumeid, sealhulgas, kuid mitte ainult:

2.3.1 sümmeetriline ja asümmeetriline krüpteerimine

2.3.2 digiallkirjad ja sertifikaadid

2.3.3 räsialgoritmid

2.3.4 võtmete turvaline genereerimine, jaotamine ja hävitamine

2.3.5 Transport Layer Security (TLS), täisketta krüpteerimine (FDE) ja API taseme krüpteerimine

2.3.6 turvalised elemendid, nagu riistvaralised turbemoodulid (HSM), Trusted Platform Module'id (TPM) ja võtmehaldussüsteemid (KMS)

2.4 Käesolev poliitika reguleerib krüptograafia kasutamist järgmistes valdkondades:

2.4.1 andmed, mis on klassifitseeritud kui konfidentsiaalne, väga konfidentsiaalne või reguleeritud

2.4.2 autentimine ja digitaalse identiteedi kontroll

2.4.3 turvaline teabevahetus väliste osapooltega

2.4.4 võtmete hoidmise vastutus ja nelja silma põhimõtte rakendamine

3. Eesmärgid

3.1 Tagada, et krüptograafilised tehnoloogiad valitakse, kiidetakse heaks, rakendatakse ja hallatakse vastavalt äririskile, rahvusvahelistele standarditele ja regulatiivsetele nõuetele.

3.2 Kehtestada standardiseeritud juhtimismudel krüptograafiateenuste haldamiseks, sealhulgas selge vastutus rakendamise, valideerimise ja erandite käsitlemise eest.

3.3 Vältida krüptograafiliste algoritmide ja kontrollimeetmete loata kasutamist, väärkonfigureerimist või aegumist ametliku heakskiitmise ja läbivaatamise protsessi kaudu.

3.4 Tagada, et krüptograafilised kontrollimeetmed integreeritakse süsteemide kavandamise etappi ja valideeritakse regulaarselt, et vältida andmete avaldumist, võtmete kompromiteerimist või protokollide nõrgenemist.

3.5 Rakendada kõigi krüptograafiliste võtmete elutsükli haldust, sealhulgas genereerimist, säilitamist, kasutamist, roteerimist, kehtetuks tunnistamist ja turvalist hävitamist.

3.6 Täita rahvusvahelisi ja piirkondlikke regulatiivseid nõudeid, mis kohustavad kasutama krüpteerimist ja turvalist andmekäitlust, sealhulgas GDPRi, DORAt, NIS2 ja COBIT 2019.

4. Rollid ja vastutused

4.1 infoturbe juht

4.1.1 Vastutab käesoleva poliitika eest ja tagab selle kooskõla ISMSiga ning ISO/IEC 27001 lisa A kontrollimeetme 8.24 nõuetega.

4.1.2 Kiidab heaks krüptograafiliste algoritmide ja kontrollimeetmete kasutamise ning tagab poliitika järgimise kogu organisatsioonis.

4.2 krüptograafiliste operatsioonide juht / turbearhitekt

4.2.1 Haldab krüptograafiliste süsteemide igapäevast käitamist ja administreerimist.

4.2.2 Hoiab ajakohasena heakskiidetud krüptograafiliste meetodite loendit (ACML) ja võtmehalduse registrit.

4.2.3 Viib läbi krüptograafilise disaini ülevaatusi (CDR) ja hindab uusi krüptograafilisi tehnoloogiaid.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Käesoleva poliitika vaatavad kord aastas läbi infoturbe juht ja krüptograafiliste operatsioonide juht.

9.2 Läbivaatamise alused hõlmavad:

9.2.1 krüptograafiliste haavatavuste avastamist (nt algoritmi nõrgenemine, kvantarvutusrünnakud)

9.2.2 regulatiivseid muudatusi, mis nõuavad ajakohastatud krüpteerimisstandardeid

9.2.3 tegevuslikke või auditileide, mis näitavad poliitika puudujääke

9.2.4 krüptograafiliste tööriistade uuendusi või arhitektuurimuudatusi

9.3 Muudatusi tuleb hallata versioonihalduse korras ISMSi dokumendikontrolli registris ja neist tuleb teavitada:

9.3.1 kõiki administraatoreid, kellel on krüptograafilised juurdepääsurollid

9.3.2 arendusmeeskondi ja DevSecOpsi juhte

9.3.3 kolmandatest osapooltest teenuseosutajaid, kellele kohalduvad lepingulised krüpteerimiskohustused

9.4 ISMSi meeskond peab tagama, et asendatud versioonid arhiveeritakse ja neile enam tegevusprotseduurides ei viidata.

10. Seotud poliitikad ja seosed

10.1 P1 - Infoturbepoliitika. Määrab kindlaks kõigi turvameetmete, sealhulgas krüptograafiliste kontrollimeetmete rakendamise, varade kaitse ja turvalise teabevahetuse alused.

10.2 P4 - Juurdepääsukontrolli poliitika. Tagab, et loogiline juurdepääs krüptograafilisele materjalile ja krüpteerimise haldussüsteemidele on rangelt piiratud vähimate õiguste põhimõtte ja ülesannete lahususe alusel.

10.3 P6 - Riskijuhtimise poliitika. Toetab krüptograafiliste kontrollimeetmetega seotud riskide hindamist ja dokumenteerib riskikäsitluse strateegia erandite, algoritmide aegumise või võtmete kompromiteerimise stsenaariumide jaoks.

10.4 P12 - Varahalduse poliitika. Nõuab tundlike andmete ja riistvaravarade klassifitseerimist, mis määrab otseselt krüptograafilised nõuded ja võtmehoidmise kohustused.

10.5 P13 - Andmete klassifitseerimise ja märgistamise poliitika. Määratleb klassifitseerimistasemed (nt konfidentsiaalne, reguleeritud), mis käivitavad konkreetsed krüpteerimisnõuded edastamisel ja puhkeolekus.

10.6 P14 - Andmete säilitamise ja kõrvaldamise poliitika. Määratleb protseduurid krüpteeritud andmekandjate ja krüptograafilise võtmematerjali turvaliseks kõrvaldamiseks elutsükli lõpus.

10.7 P30 - Intsidendihalduse poliitika (P30). Kirjeldab organisatsiooni reageerimisstrateegiat võtmete kompromiteerimise, sertifikaatide väärkasutuse või algoritmiliste haavatavuste kahtluse korral, sealhulgas kiiret kehtetuks tunnistamist ja rikkumisest teavitamist.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 8.1 - tegevuste planeerimine ja kontroll: nõuab tehniliste turbekontrollide, sealhulgas krüptograafiliste meetmete rakendamist osana tegevuslikest kaitsemeetmetest.

11.2 ISO/IEC 27002:2022

11.2.1 Kontrollimeetmed 8.24, 8.25, 8: annavad rakendussuunised krüptograafiliste kontrollimeetmete eesmärkide, algoritmide valiku, protokollide rakendamise ja sertifikaatide elutsükli halduse kohta.

11.3 NIST SP 800-53 Rev.

11.3.1 SC-12 - krüptograafiliste võtmete loomine: tagab krüpteerimisvõtmete turvalise genereerimise ja vahetamise. P18 määratleb, kuidas sümmeetrilisi ja asümmeetrilisi võtmeid tuleb genereerida ja vahetada heakskiidetud algoritmide ja protokollide abil.

11.3.2 SC-13 - krüptograafiline kaitse: nõuab krüptograafia kasutamist teabe konfidentsiaalsuse ja tervikluse kaitsmiseks. P18 nõuab andmete krüpteerimist puhkeolekus ja edastamisel vastavalt andmete klassifitseerimisele, kus algoritmistandardid on kooskõlas NISTi FIPS 140-3ga.

11.3.3 SC-17 - avaliku võtme taristu (PKI) sertifikaadid: nõuab PKI rakendamist autentimise ja digiallkirjade toetamiseks. P18 kirjeldab PKI kasutamist teabevahetuse, süsteemiidentiteetide ja haldusjuurdepääsu kaitsmiseks.

11.3.4 SC-28, SC-28(1) - teabe kaitse puhkeolekus ja edastamisel: nõuab andmete krüpteerimist nende säilitamisel või edastamisel mitteusaldusväärsete võrkude kaudu. P18 määratleb TLSi, VPN-tunnelite, täiskettakrüpteerimise ja tundlike andmete turvaliste säilitamismeetodite rakendamise.

11.3.5 SC-12(3) - sümmeetriliste võtmete genereerimine turvaliseks säilitamiseks ja jaotamiseks: keskendub sümmeetriliste võtmete turvalisele genereerimisele ja käsitlemisele. P18 nõuab tugevate juhuarvugeneraatorite kasutamist, võtmete roteerimise poliitikaid ja turvalisi võtmehoidlaid krüptograafiliste toimingute jaoks.

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

11.4.1 Artikkel 32 - töötlemise turvalisus: soovitab sõnaselgelt krüpteerimist isikuandmete riskide vähendamise meetmena.

11.4.2 Põhjendus 83: rõhutab krüpteerimist kontrollimeetmena, mis aitab vältida loata juurdepääsu andmetele.

11.4.3 Artiklid 33 ja 34: tõhus krüpteerimine võib vabastada organisatsiooni kohustusest rikkumisest teavitada.

11.5 ELi NIS2 direktiiv (2022/2555)

11.5.1 Artikkel 21(2)(d): nõuab tehnilisi ja korralduslikke meetmeid, sealhulgas krüptograafilisi kaitsemeetmeid, teenuse käideldavuse ja tervikluse säilitamiseks.

11.6 ELi DORA (2022/2554)

11.6.1 Artikkel 6(2)(d): finantsasutused peavad andmeid kaitsma, sealhulgas kriitilise teabe tugeva krüpteerimise kaudu.

11.6.2 Artikkel 11(1)(c): nõuab IKT kolmandatest osapooltest teenuseosutajate jaoks turvalisi andmetöötluse kontrollimeetmeid.

11.7 COBIT 2019

11.7.1 DSS05.01 - teabevarade kaitsmine: nõuab krüpteerimise ja võtmehalduse kasutamist andmete kaitsmiseks loata juurdepääsu eest.

11.7.2 DSS06.06 - hallatud turbetestimine: soovitab krüptograafilise vastavuse valideerimist haavatavuste hindamise osana.

11.7.3 MEA03 - vastavuse seire, hindamine ja auditeerimine: nõuab krüptograafiliste kontrollimeetmete tõhususe pidevat tagamist.