					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P31					Dokumendi pealkiri: **Tõendite kogumise ja kohtuekspertiisi 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 õigusnormidega

Standard/õigusnorm	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 8	
ISO/IEC 27002:2022	Kontrollimeetmed 5.25–5.27, 8.27	
ISO/IEC 27035:2016	Osad 1 ja 3	
NIST SP 800-53 Rev. 5	IR-1 kuni IR-9, AU-6, PL-2	
NIST SP 800-101 Rev. 1	Mobiilseadmete ja andmekandjate kohtuekspertiis	Mobiilseadmete ja andmekandjate kohtuekspertiis
NIST SP 800-86	Kohtuekspertiisi meetodite lõimimine	Kohtuekspertiisi meetodite lõimimine intsidentidele reageerimisse
ELi isikuandmete kaitse üldmäärus (GDPR)	Artikkel 5, 33–34	
ELi NIS2 direktiiv	Artikkel 23(1)–(4)	
ELi DORA	Artikkel 17(1)–(3)	
COBIT 2019	DSS01.07, DSS05.04	

1. Eesmärk

1.1 Käesolev poliitika kehtestab struktureeritud ja õiguslikult kaitstava raamistiku digitaalse tõendusmaterjali tuvastamiseks, kogumiseks, säilitamiseks, analüüsimiseks ja hävitamiseks tegelike või kahtlustatavate turvaintsidentide korral.

1.2 See tagab, et kohtuekspertiisiks valmisoleku ja tõendite käitlemise protsessid:

1.2.1 säilitavad tõendusmaterjali tervikluse ja tõendite valduse ahela;

1.2.2 toetavad sisejuurdlusi, kohtumenetlusi või regulatiivset teavitamist;

1.2.3 on kooskõlas rahvusvaheliselt tunnustatud kohtuekspertiisi standardite ja õigusliku vastuvõetavuse kriteeriumidega.

1.3 Käesolev poliitika toetab organisatsiooni kohustust rakendada ennetavat intsidentidele reageerimist, täita õiguslikke kohustusi ja tagada juhtimise läbipaistvus, minimeerides samal ajal tegevushäireid.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib järgmiste isikute ja objektide suhtes:

2.1.1 kõik töötajad, töövõtjad, tarnijad ja teenuseosutajad, kes osalevad süsteemihalduses, intsidentide käsitlemises või juurdlustoimingutes;

2.1.2 kõik lõppseadmed, serverid, rakendused, võrgud ja pilveplatvormid, mis on organisatsiooni kontrolli või lepingulise vastutuse all;

2.1.3 kõik intsidendid või sündmused, mis nõuavad tõendite käitlemist, sealhulgas:

2.1.3.1 siseohud, andmekaitserikkumised või pettusejuurdlused;

2.1.3.2 süsteemide või autentimisandmete väärkasutus;

2.1.3.3 operatsioonitehnoloogia (OT) või tööstusjuhtimissüsteemide intsidendid;

2.1.3.4 füüsilise juurdepääsu rikkumised, mis hõlmavad digitaalseid varasid.

2.2 Käesolev poliitika reguleerib ka suhtlust kolmandatest isikutest kohtuekspertiisiteenuse osutajate või õiguskaitseasutustega õigusliku või regulatiivse eskaleerimise või menetluste korral.

3. Eesmärgid

3.1 Võimaldada kiiret, turvalist ja poliitikaga kooskõlas olevat tõendite kogumist turvasündmuste või juurdluste käigus.

3.2 Säilitada kogutud digitaalse tõendusmaterjali terviklus, autentsus ja vastuvõetavus range juurdepääsukontrolli, logimise ja verifitseerimisprotseduuride kaudu.

3.3 Tagada, et kõik kohtuekspertiisi tegevused on kooskõlastatud õiguslike ja regulatiivsete kohustustega, sealhulgas andmekaitse, tööõiguse ja rahvusvaheliste andmeedastuspiirangutega.

3.4 Toetada intsidendijärgset analüüsi, algpõhjuse analüüsi ja kontrollimeetmete täiustamist kvaliteetse kohtuekspertiisi väljundi kaudu.

3.5 Lõimida kohtuekspertiisiks valmisolek üldisesse infoturbe juhtimissüsteemi (ISMS) raamistikku, toetades auditeid, rikkumiste teavitamist ja juhtkonna otsuste tegemist.

4. Rollid ja vastutused

4.1 Infoturbe juht

4.1.1 Vastutab käesoleva poliitika eest ning tagab, et kõik kohtuekspertiisi toimingud on õiguslikult kaitstavad, auditikõlblikud ja riskipõhised.

4.1.2 Annab loa eskaleerimiseks välistele õigusnõustajatele, ametiasutustele ja kohtuekspertiisiteenuse osutajatele.

4.2 Kohtuekspertiisi analüütikud / intsidentide käsitlejad

4.2.1 Juhivad tõendite kogumist, säilitamist ja tehnilist analüüsi.

4.2.2 Tagavad, et tõendite valduse ahel on nõuetekohaselt dokumenteeritud ja säilitatud.

4.2.3 Dokumenteerivad kõik juurdluse käigus tehtud toimingud, leiud ja kasutatud tööriistade seadistused.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Käesolev poliitika tuleb vähemalt kord aastas läbi vaadata ja vajaduse korral ajakohastada, et arvestada järgmisega:

9.1.1 muudatused seadustes, määrustes või kohtupraktikas, mis mõjutavad kohtuekspertiisi protseduure või andmekäitlust;

9.1.2 uuendused valdkonnas tunnustatud kohtuekspertiisi standardites või tööriistades;

9.1.3 intsidendijärgsetest ülevaatustest, õigusvaidlustest või auditileidudest saadud õppetunnid;

9.1.4 tehnoloogilised muudatused uuritavates platvormides, seadmetes või süsteemides.

9.2 Läbivaatamise protsessi eest vastutab infoturbe juht ning see peab hõlmama konsulteerimist järgmiste osapooltega:

9.2.1 õigus- ja vastavusfunktsioon;

9.2.2 andmekaitseametnik (DPO);

9.2.3 turbeoperatsioonide ja kohtuekspertiisi meeskonnad;

9.2.4 siseaudit.

9.3 Kõik muudatused peavad olema:

9.3.1 versioonihalduse all ja talletatud poliitikate keskhoidlas;

9.3.2 edastatud mõjutatud sidusrühmadele, sealhulgas kohtuekspertiisi- ja reageerimismeeskondadele;

9.3.3 kajastatud asjakohastes tööjuhendites ja koolitusmaterjalides.

9.4 Vahepealsed läbivaatused tuleb algatada pärast mis tahes kriitilist intsidenti, mis hõlmab tõendusmaterjali mittenõuetekohast käitlemist, tõendite valduse ahela tõrget või õigusliku vastuvõetavuse probleeme.

10. Seotud poliitikad ja seosed

10.1 Käesolev poliitika on kooskõlas järgmiste organisatsiooni poliitikatega ja neid toetab:

10.1.1 P1 – Infoturbepoliitika: kehtestab juurdluste, tõendite kontrolli ja kohaldatavate õigusaktide järgimise põhialused.

10.1.2 P5 – Muudatuste haldamise poliitika: tagab, et uurimise all olevaid süsteeme ei muudeta aktiivsete kohtueksperti isi protsesside ajal.

10.1.3 P14 – Andmete säilitamise ja hävitamise poliitika: reguleerib tõendite ja juhtumiga seotud andmete turvalist hävitamist ning säilitustähtaegu.

10.1.4 P18 – Krüptograafiliste kontrollimeetmete poliitika: kehtestab tundlike või tõendusliku väärtusega andmete säilitamise ja edastamise krüptimisnõuded.

10.1.5 P22 – Logimise ja seire poliitika: tagab sündmuslogide ja telemeetria kättesaadavuse tõendite kogumiseks ja kohtueksperti isi korrelatsiooniks.

10.1.6 P30 – Intsidentidele reageerimise poliitika: määratleb intsidentide esmase hindamise ja eskaleerimisteed, mille korral käivitatakse kohtueksperti isi protseduurid.

10.1.7 P33 – Auditi ja vastavuse seire poliitika: valideerib regulaarsete auditite kaudu kohtueksperti isi protokollide ja tõendite valduse ahela nõuete järgimist.

11. Viitestandardid ja raamistikud

11.1 Käesolev poliitika on kooskõlas rahvusvaheliste kohtueksperti isi ja intsidentide käsitlemise standarditega, tagades tõendusmaterjali tervikluse, õigusliku kaitstavuse ja piiriülese vastavuse.

11.2 ISO/IEC 27001

11.2.1 Punkt 8.1 – toetab kohtueksperti isiks valmisoleku ja tõendite käitlemise protseduuride operatiivjuhtimist.

11.3 ISO/IEC 27002

11.3.1 Lisa A kontroll 5.25 – Intsidendihalduse vastutused: nõuab infoturbeintsidentide ja juurdluste käsitlemiseks määratletud rolle.

11.3.2 Lisa A kontroll 5.26 – Infoturbe sündmustest teatamine: toetab sündmustega seotud artefaktide kogumist tõendusmaterjalina.

11.3.3 Lisa A kontroll 5.27 – Reageerimine infoturbeintsidentidele: nõuab struktureeritud, tõenduspõhist ohjamist ja uurimist.

11.3.4 Lisa A kontroll 8.27 – Turvaline arendus ja kohtueksperti is (kui asjakohane): käsitleb süsteemide ja tööriistade kaitset juurdluste ajal.

11.4 ISO/IEC 27035:2016 (osad 1 ja 3)

11.4.1 Määratleb intsidentide tuvastamise, reageerimise ja kohtueksperti isiks valmisoleku põhimõtted, sealhulgas planeerimise, tõendite valduse ahela ja intsidendiga seotud tõendusmaterjali haldamise.

11.5 NIST SP 800-53 Rev. 5

11.5.1 IR-1 kuni IR-9, AU-6, PL-2: määratleb struktureeritud nõuded turvaintsidentide planeerimiseks, tuvastamiseks, analüüsimiseks, ohjeldamiseks ja neile reageerimiseks. Toetab tõendusmaterjali kogumist ja auditikõlblikkust (AU-6) ning tagab kohtueksperti isi juurdluste ajal kooskõla süsteemi turbe- ja andmekaitseplaanidega (PL-2).

11.6 NIST SP 800-86

11.6.1 Annab juhised kohtueksperti protsesside lõimimiseks laiemasse intsidentidele reageerimise elutsüklisse ja kohtueksperti valmisoleku tagamiseks.

11.7 NIST SP 800-101 Rev. 1

11.7.1 Keskendub parimatele praktikatele digitaalsete andmekandjate ja mobiilseadmete tõendusmaterjali kogumisel, säilitamisel ja analüüsimisel õiguslikult kaitstaval viisil.

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

11.8.1 Artikkel 5 – Isikuandmete töötlemise põhimõtted: kohaldub tõendusmaterjalile, mis sisaldab isikuandmeid või tundlikke andmeid, tagades andmete minimaalsuse ja eesmärgipärasuse.

11.8.2 Artiklid 33–34 – andmekaitserikkumisest teavitamine: kohtueksperti andmed toetavad vastavust rikkumiste teavitamise kohustustele ja õigusliku avalikustamise protsessidele.

11.9 ELi NIS2 direktiiv (2022/2555)

11.9.1 Artikkel 23 – teavitamiskohustused: kohtueksperti dokumentatsioon ja leiud toetavad pädevatele asutustele esitatavaid õigeaegseid ja täpseid intsidendiaruandeid.

11.10 ELi DORA (2022/2554)

11.10.1 Artikkel 17 – IKT-intsidentidest teavitamine: nõuab oluliste IKTga seotud intsidentide üksikasjalikku algpõhjuse analüüsi ja tõendavaid kirjeid, eriti finantssektoris.

11.11 COBIT 2019

11.11.1 DSS01.07 – Turvaintsidentide haldamine: nõuab intsidentide dokumenteerimist ja uurimise põhjalikkust.

11.11.2 DSS05.04 – Turbejuurdluste haldamine: rõhutab digitaalse tõendusmaterjali säilitamist ning toetust distsiplinaar- ja õiguslikele meetmetele.