					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P31S					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**

Õiguslik teatis (autoriõigus ja kasutuspiirangud)

(C) 2025 Clarysec LLC. All rights reserved.

Käesolev dokument on Clarysec LLC intellektuaalomand. Selle dokumendi ühtegi osa ei tohi ilma eelneva selgesõnalise kirjaliku loata kopeerida, taaskasutada, levitada ega muuta ärilistel või rakendamise eesmärkidel.

Loata kasutamine on rangelt keelatud ja võib kaasa tuua õiguslikke meetmeid.

Litsentsimise küsimustes võtke ühendust: info@clarysec.com

Kooskõla standardite ja õigusaktidega

Standard/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punktid 6.1, 6.3, 8	Riskipõhine planeerimine, parendustegevused ja operatiivsed ohjemeetmed tõendite tervikluse tagamiseks
ISO/IEC 27002:2022	Ohjemeetmed 5.24–5.27	Juhendavad turvalist käitlemist, intsidendijärgseid ülevaatusi ja tõendipõhiseid parendusi
ISO/IEC 27035-3:2016	Punktid 6.3, 6.4, 7	Tagab digitaalse tõendusmaterjali nõuetekohase planeerimise, õiguspärase kogumise ja turvalise käitlemise koos valduse ahela dokumenteerimisega
NIST SP 800-53 Rev.5	IR-07, IR-08, AU-09, AU-12, PE-18	Kohtueksperti isivalmidus, auditilogide kaitse ja tõendite kogumise tõhus lõimimine intsidentidele reageerimisse
EL GDPR	Artiklid 33, 34	Isikuandmetega seotud rikkumiste dokumenteerimine ja jälgitavus
EL NIS2	Artikkel 23	Jälgitav intsidentidest teatamine ja tõendite turvaline käitlemine
EL DORA	Artikkel 17(1), 17(2)	Tagab IKT-ga seotud intsidentide tõendite kogumise, säilitamise ja hoidmise, kohtueksperti isilise usaldusväärsuse ning toetab regulatiivseid päringuid
COBIT 2019	DSS05.06, DSS05.07	Usaldusväärne logimine ja struktureeritud tõendite käitlemine turvalisteks, auditikõlblikeks uurimisteks

1. Eesmärk

1.1. Käesolev poliitika määratleb, kuidas organisatsioon käitleb turvaintsidentide, isikuandmete rikkumiste või sisejuurdlustega seotud digitaalset tõendusmaterjali. Poliitika tagab, et tõendusmaterjali kogutakse, säilitatakse ja hoitakse viisil, mis on õiguslikult põhjendatud ja auditiks valmis ning toetab nii organisatsioonisisest otsustamist kui ka võimalikke väliseid menetlusi.

1.2. Poliitika võimaldab väikestel organisatsioonidel kaitsta logide, failide ja süsteemikujutiste terviklust ning tõendada hoolsuskohustuse täitmist ISO/IEC 27001, GDPR-i ja seotud standardite alusel.

1.3. Poliitika toetab kohtueksperti isivalmidust ilma vajaduseta kasutada keerukaid tehnilisi ressursse või täiskohaga IT-meeskonda, määratledes selged rollid ja vastutused, protsessid ning säilitamisnõuded.

2. Kohaldamisala

2.1. Käesolev poliitika kehtib järgmistele osapooltele ja vahenditele:

2.1.1. kõik töötajad, IT-teenuse osutajad ja väliskonsultandid, kes osalevad intsidentidele reageerimises, uurimises või rikkumiste analüüsis;

2.1.2. kõik ettevõtte süsteemid, sealhulgas sülearvutid, mobiilsed seadmed, serverid, e-posti kontod, SaaS-platvormid ja pilvesalvestuslahendused (nt Microsoft 365, Google Workspace);

2.1.3. kõik sündmused, mille puhul on tõendusmaterjal vajalik sisemiste distsiplinaarmeetmete, õigusliku kaitse, kahjunõuete või reguleerivate asutustega suhtlemise jaoks.

2.2. Poliitika hõlmab nii tegelikke kui ka kahtlustatavaid sündmusi, mis on seotud järgmisega:

2.2.1. andmeleke;

2.2.2. siseoht või väärkasutus;

2.2.3. turvarikkumised (nt pahavara, loata juurdepääs);

2.2.4. kliendikaebused, mis nõuavad digitaalset kinnitamist;

2.2.5. reguleerivate asutuste või õiguskaitseasutuste päringud.

3. Eesmärgid

3.1. Tagada, et kogu tõendusmaterjal kogutakse ja käideldakse viisil, mis säilitab selle tervikluse, autentsuse ja valduse ahela.

3.2. Vältida logide, failide või süsteemikujutiste juhuslikku muutmist, kustutamist või väära käitlemist, kui neid võib olla vaja uurimiseks.

3.3. Kehtestada ühtne ja auditikõlblik lähenemine tõendusmaterjali haldamisele, mis vastab õiguslikele ja regulatiivsetele ootustele (nt GDPR-i rikkumiste teavitamine, NIS2 jälgitavus).

3.4. Määratleda selged rollid ja vastutused, et tagada turvaintsidentide ajal tõendusmaterjali kiire, turvaline ja õigusnõuetele vastav kogumine.

3.5. Toetada VKE tasemel kohtuekspertiisivalmidust, minimeerides keerukust ja vältides häireid igapäevases tegevuses.

4. Rollid ja vastutused

4.1. tegevjuht

4.1.1. kiidab heaks kõik ametlikud uurimised, mis nõuavad tõendusmaterjali kogumist;

4.1.2. vaatab läbi ja kinnitab intsidendiaruanded, mis hõlmavad võimalikke õiguslikke või distsiplinaarmeetmeid;

4.1.3. otsustab, kas tuleb teavitada välist õigusnõustajat või reguleerivaid asutusi;

4.1.4. tagab poliitika regulaarse läbivaatamise ja ajakohastamise.

4.2. IT-teenuse osutaja / süsteemiadministraator

4.2.1. kogub ja säilitab digitaalset tõendusmaterjali turvaliste protseduuride kohaselt;

4.2.2. dokumenteerib ajamärgid, süsteemi üksikasjad ja käitlemise etapid;

4.2.3. tagab kogu kogutud materjali hoidmise kaitstud asukohas;

4.2.4. toetab vajaduse korral kohtuekspertiisilist analüüsi.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1. Poliitika iga-aastane läbivaatamine

9.1.1. tegevjuht peab käesoleva poliitika vähemalt kord 12 kuu jooksul läbi vaatama, et kinnitada:

9.1.1.1. vastavus ISO/IEC 27001 lisa A ohjemeetmetele;

9.1.1.2. jätkuv asjakohasus kehtivate digitaalsete platvormide ja IT-teenuste suhtes;

9.1.1.3. logimise, tõendusmaterjali säilitamise ja kohtuekspertiisivalmiduse protseduuride piisavus.

9.2. Poliitika muutmise alused

9.2.1. poliitika tuleb läbi vaadata ja ajakohastada ka pärast järgmist:

9.2.1.1. iga oluline intsident, mis nõuab tõendusmaterjali kogumist;

9.2.1.2. ebaõnnestunud audit või regulatiivne päring, mille käigus seati kahtluse alla tõendusmaterjali terviklus;

9.2.1.3. uute tööriistade või protseduuride kasutuselevõtt intsidentidele reageerimiseks või süsteemide seireks;

9.2.1.4. õiguslikud muudatused (nt ajakohastatud GDPR-i või NIS2 suunised).

9.3. Muudatuste heakskiitmine ja edastamine

9.3.1. kõik muudatused peab läbi vaatama ja heaks kiitma tegevjuht;

9.3.2. ajakohastatud versioon tuleb edastada järgmistele osapooltele:

9.3.2.1. IT-teenuse osutajad ja konsultandid, kes osalevad uurimistes;

9.3.2.2. töötajad, kellel on süsteemiadministreerimise vastutus.

9.3.3. ajakohastatud koopia tuleb säilitada ettevõtte poliitikaarhiivis ja teha see nõudmisel audiitoritele kättesaadavaks.

10. Seotud poliitikad ja seosed

10.1. Käesolev poliitika on vastastikku seotud järgmiste VKE-le kohandatud poliitikatega:

10.1.1. P2S – Juhtimisrollide ja vastutuste poliitika: määratleb volitused intsidendiuurimiste, tõenditega seotud otsuste ja õigusliku eskaleerimise üle.

10.1.2. P4S – Juurdepääsukontrolli poliitika: tagab, et uurimiste ajal pääsevad tundlikele süsteemidele ja logidele ligi ainult volitatud isikud.

10.1.3. P22S – Logimise ja seire poliitika: määratleb kohtuekspertiisilise tõendusmaterjali lähteandmed ning säilitamise, juurdepääsukontrolli ja logimise nõuded.

10.1.4. P30S – Intsidentidele reageerimise poliitika: käivitab tõendusmaterjali kogumise vajaduse ja määratleb operatiivse voo, mis viib kohtuekspertiisilise säilitamiseni.

10.1.5. P17S – Andmekaitse ja privaatsuse poliitika: tagab, et tõendusmaterjalina kogutud isikuandmeid käideldakse õiguspäraselt GDPR-i ja seotud õigusaktide alusel.

10.2. Need poliitikad toimivad koos, et tagada õiguslik kaitstavus, uurimise terviklus ja täielik auditivalmidus kooskõlas standardiga ISO/IEC 27001:2022.

11. Viitestandardid ja raamistikud

11.1. ISO/IEC 27001

11.1.1. Punkt 6.1 – riskipõhine planeerimine hõlmab reageerimisvalmidust ja tõenditega seotud protseduure.

11.1.2. Punkt 6.3 – toetab intsidenditõenditel põhinevaid parendustegevusi.

11.1.3. Punkt 8.1 – nõuab operatiivseid ohjemeetmeid tõendite tervikluse tagamiseks.

11.2. ISO/IEC 27002

11.2.1. Ohjemeetmed 5.24–5.27 – juhendavad turvalist käitlemist, intsidendijärgseid ülevaatusi ja tõendipõhiseid parendusi.

11.3. ISO/IEC 27035-3

11.3.1. Punktid 6.3, 6.4 ja 7.3 tagavad digitaalse tõendusmaterjali nõuetekohase planeerimise, õiguspärase kogumise ja turvalise käitlemise intsidentidele reageerimise ajal, sealhulgas säilitamise ja valduse ahela dokumenteerimise.

11.4. NIST SP 800-53 Rev. 5

11.4.1. IR-07, IR-08, AU-09 ja AU-12 tagavad kohtuekspertiisivalmiduse, auditilogide kaitse ja tõendite kogumise tõhusa lõimimise intsidentidele reageerimise elutsüklisse.

11.5. NIST SP 800-86

11.5.1. Määratleb digitaalse tõendusmaterjali kogumise, analüüsimise ja kaitsmise head tavad intsidentidele reageerimise käigus.

11.6. EL GDPR

11.6.1. Artiklid 33–34 – nõuavad intsidendide ja tõendusmaterjali dokumenteerimist ning jälgitavust isikuandmete rikkumistest teatamisel.

11.7. EL NIS2 direktiiv (2022/2555)

11.7.1. Artikkel 23 – nõuab elutähtsatelt ja olulistelt üksustelt jälgitavat intsidentidest teatamist ja tõendite turvalist käitlemist.

11.8. EL DORA

11.8.1. Artikkel 17(1) – tagab, et IKT-ga seotud intsidentidega seotud tõendusmaterjal kogutakse ja säilitatakse viisil, mis toetab kohtuekspertiisilisi uurimisi.

11.8.2. Artikkel 17(2) – nõuab, et finantssektori üksused säilitaksid kõik turvasündmustega seotud asjakohased andmed ja logid kooskõlas kohtuekspertiisilise usaldusväärsuse ning regulatiivsete päringute nõuetega.

11.9. COBIT 2019

11.9.1. DSS05.06 – intsidentide seire, tuvastamine ja teatamine: rõhutab usaldusväärse logimise tähtsust uurimiste toetamisel.

11.9.2. DSS05.07 – intsidentide uurimine ja meetmete rakendamine: nõuab struktureeritud tõendite käitlemist, et võimaldada turvalisi ja auditikõlblikke uurimisi.