					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P31					Asiakirjan nimi: **Todistusaineiston keräämisen ja forensiikan politiikka**							
Versio: 1.0		Voimaantulopäivä: 01.01.2025			Asiakirjan omistaja:							
X	Politiikka		Standardi		Menettely		Lomake		Rekisteri		Muu	

Muutoshistoria				
Muutosnumero	**Muutospäivä**	**Muutokset**	**Tarkistanut**	**Prosessin omistaja**

Hyväksynnät			
Nimi	**Tehtävänimike**	**Päivämäärä**	**Allekirjoitus**

Yhdenmukaisuus standardien ja sääntelyvaatimusten kanssa

Standardi/sääntely	Lauseke/artikla	Kommentti
ISO/IEC 27001:2022	Lauseke 8	
ISO/IEC 27002:2022	Kontrollit 5.25–5.27, 8.27	
ISO/IEC 27035:2016	Osat 1 ja 3	
NIST SP 800-53 Rev.5	IR-1–IR-9, AU-6, PL-2	
NIST SP 800-101 Rev.1	Mobiili- ja tietovälineforensiikka	Mobiili- ja tietovälineforensiikka
NIST SP 800-86	Forensisten tekniikoiden integrointi	Forensisten tekniikoiden integrointi tietoturvapoikkeamiin reagointiin
EU:n GDPR	Artikla 5, 33–34	
EU:n NIS2-direktiivi	Artikla 23(1)–(4)	
EU:n DORA-asetus	Artikla 17(1)–(3)	
COBIT 2019	DSS01.07, DSS05	

1. Tarkoitus

1.1 Tällä politiikalla määritetään jäsennelty ja oikeudellisesti puolustettava viitekehys digitaalisen todistusaineiston tunnistamiseen, keräämiseen, säilyttämiseen, analysointiin ja hävittämiseen toteutuneiden tai epäiltyjen tietoturvapoikkeamien yhteydessä.

1.2 Tällä varmistetaan, että forensinen valmius ja todistusaineiston käsittelyprosessit:

1.2.1 säilyttävät todistusaineiston eheyden ja hallussapitoketjun

1.2.2 tukevat sisäisiä tutkintoja, oikeudenkäyntejä ja viranomaisraportointia

1.2.3 ovat yhdenmukaisia kansainvälisesti hyväksyttyjen forensiikkastandardien ja oikeudellisen hyväksyttävyyden kriteerien kanssa

1.3 Politiikka tukee organisaation sitoutumista ennakoivaan tietoturvapoikkeamien käsittelyyn, vaatimustenmukaisuuteen ja hallinnon läpinäkyvyyteen sekä minimoi toiminnalliset häiriöt.

2. Soveltamisala

2.1 Tämä politiikka koskee:

2.1.1 kaikkia työntekijöitä, urakoitsijoita, toimittajia ja palveluntarjoajia, jotka osallistuvat järjestelmähallintaan, poikkeamien käsittelyyn tai tutkintatoimintaan

2.1.2 kaikkia päätelaitteita, palvelimia, sovelluksia, verkkoja ja pilvialustoja, jotka ovat organisaation hallinnassa tai sopimusvastuulla

2.1.3 kaikkia poikkeamia tai tapahtumia, jotka edellyttävät todistusaineiston käsittelyä, mukaan lukien:

2.1.3.1 sisäiset uhat, tietomurrot tai petostutkinnat

2.1.3.2 järjestelmien tai tunnistetietojen väärinkäyttö

2.1.3.3 operatiiviseen teknologiaan (OT) tai teollisiin ohjausjärjestelmiin liittyvät poikkeamat

2.1.3.4 fyysisen pääsyn rikkomukset, jotka kohdistuvat digitaalisiin omaisuuseriin

2.2 Politiikka ohjaa myös kaikkea yhteistyötä kolmannen osapuolen forensiikkapalvelujen tai lainvalvontaviranomaisten kanssa lakisääteisten ja sääntelyyn liittyvien eskalointien tai viranomaismenettelyjen yhteydessä.

3. Tavoitteet

3.1 Mahdollistaa nopea, turvallinen ja politiikan mukainen todistusaineiston hankinta tietoturvatapahtumien tai tutkintojen aikana.

3.2 Säilyttää kerätyn digitaalisen todistusaineiston eheys, aitous ja hyväksyttävyys tiukan pääsynhallinnan, lokituksen ja varmennusmenettelyjen avulla.

3.3 Varmistaa, että kaikki forensiset toiminnot sovitetaan yhteen lakisääteisten ja sääntelyyn perustuvien velvoitteiden kanssa, mukaan lukien tietosuoja, työoikeus ja kansainvälisiä siirtoja koskevat rajoitukset.

3.4 Tukea poikkeaman jälkeistä analyysiä, juurisyyanalyysiä ja kontrollien parantamista laadukkaiden forensisten tuotosten avulla.

3.5 Integroida forensinen valmius osaksi tietoturvallisuuden hallintajärjestelmää (ISMS) auditointien, loukkausilmoitusten ja ylimmän johdon päätöksenteon tueksi.

4. Roolit ja vastuut

4.1 Tietoturvajohtaja (CISO)

4.1.1 Omistaa tämän politiikan ja varmistaa, että kaikki forensiset toiminnot ovat oikeudellisesti puolustettavia, todennettavia ja riskiperusteisia.

4.1.2 Valtuuttaa eskaloinnin ulkoisille oikeudellisille tahoille ja forensiikkapalveluntarjoajille.

4.2 Forensiset analyytikot / poikkeamankäsittelijät

4.2.1 Vastaavat todistusaineiston hankinnan, säilyttämisen ja teknisen analyysin johtamisesta.

4.2.2 Varmistavat, että hallussapitoketju dokumentoidaan asianmukaisesti ja säilytetään.

4.2.3 Dokumentoivat kaikki tutkinnan aikana tehdyt toimet, havainnot ja käytettyjen työkalujen asetukset.

[... Jaksot 4.3–8 eivät sisälly tähän esikatseluun. Osta koko asiakirja saadaksesi täyden sisällön. ...]

9. Katselmointi- ja päivitysvaatimukset

9.1 Tämä politiikka on katselmoitava vähintään vuosittain ja päivitettävä tarvittaessa vastaamaan:

9.1.1 muutoksia laeissa, sääntelyssä tai oikeuskäytännössä, jotka vaikuttavat forensisiin menettelyihin tai tietojen käsittelyyn

9.1.2 toimialalla tunnustettujen forensiikkastandardien tai työkalujen päivityksiä

9.1.3 poikkeamien jälkiarvioinneista, oikeudellisista riidoista tai auditointihavainnoista saatuja oppeja

9.1.4 tutkinnan kohteena oleviin alustoihin, laitteisiin tai järjestelmiin kohdistuvia teknologisia muutoksia

9.2 Katselmointiprosessin omistaa tietoturvajohtaja (CISO), ja siihen on sisällyttävä seuraavien tahojen kuuleminen:

9.2.1 lakiasiat ja vaatimustenmukaisuus

9.2.2 Tietosuojavastaava (DPO)

9.2.3 tietoturvaoperaatiot ja forensiikkatiimit

9.2.4 sisäinen tarkastus

9.3 Kaikkien muutosten on oltava:

9.3.1 versionhallittuja ja tallennettuja politiikkatietovarantoon

9.3.2 viestittyjä vaikutuksen kohteena oleville sidosryhmille, mukaan lukien forensiikka- ja reagointitiimit

9.3.3 täydennettyjä asiaankuuluvien toimintamenettelyjen ja koulutusmateriaalien päivityksillä

9.4 Välitön katselmointi on käynnistettävä minkä tahansa kriittisen poikkeaman jälkeen, johon liittyy todistusaineiston virheellinen käsittely, hallussapitoketjun epäonnistuminen tai oikeudelliseen hyväksyttävyyteen liittyviä ongelmia.

10. Liittyvät politiikat ja yhteydet

10.1 Tämä politiikka on yhdenmukainen seuraavien organisaation politiikkojen kanssa, ja niitä sovelletaan sitä tukevasti:

10.1.1 P1 – Tietoturvapolitiikka: määrittää tutkintojen, todistusaineiston hallinnan ja soveltuvien lakien noudattamisen perustan.

10.1.2 P5 – Muutoksenhallintapolitiikka: varmistaa, ettei tutkinnan kohteena olevia järjestelmiä muuteta aktiivisten forensisten prosessien aikana.

10.1.3 P14 – Tietojen säilytys- ja hävityspolitiikka: ohjaa todistusaineiston ja tapaukseen liittyvien tietojen turvallista hävittämistä ja säilytysaikoja.

10.1.4 P18 – Kryptografisten hallintakeinojen politiikka: määrittää salausvaatimukset arkaluonteisten tai todistusarvoisten tietojen säilyttämiselle ja siirtämiselle.

10.1.5 P22 – Lokitus- ja valvontapolitiikka: varmistaa tapahtumalokien ja telemetrian saatavuuden todistusaineiston keräämistä ja forensista korrelointia varten.

10.1.6 P30 – Tietoturvapoikkeamien hallintapolitiikka: määrittää poikkeamien luokittelu- ja priorisointikäytännöt sekä eskalointipolut, joissa forensiset menettelyt käynnistyvät.

10.1.7 P33 – Auditointi- ja vaatimustenmukaisuuden seurantapolitiikka: varmentaa forensisten menettelyjen ja hallussapitoketjuvaatimusten noudattamisen säännöllisillä auditoinneilla.

11. Viitestandardit ja viitekehykset

11.1 Tämä politiikka on yhdenmukainen kansainvälisten forensiikkaa ja poikkeamien käsittelyä koskevien standardien kanssa varmistaen todistusaineiston eheyden, oikeudellisen puolustettavuuden ja eri lainkäyttöalueiden vaatimustenmukaisuuden.

11.2 ISO/IEC 27001

11.2.1 Lauseke 8.1 – tukee forensisen valmiuden ja todistusaineistomenettelyjen operatiivista hallintaa

11.3 ISO/IEC 27002

11.3.1 Liite A, kontrolli 5.25 – poikkeamien hallinnan vastuut: edellyttää määritettyjä rooleja tietoturvapoikkeamien ja tutkintojen käsittelyyn.

11.3.2 Liite A, kontrolli 5.26 – tietoturvatapahtumien raportointi: tukee tapahtumiin liittyvien artefaktien keräämistä todistusaineistoksi.

11.3.3 Liite A, kontrolli 5.27 – reagointi tietoturvapoikkeamiin: edellyttää jäsenneltyä, todistusaineistoon perustuvaa korjaamista ja tutkintaa.

11.3.4 Liite A, kontrolli 8.27 – turvallinen kehitys ja forensiikka (soveltuvin osin): käsittelee järjestelmien ja työkalujen suojaamista tutkintojen aikana.

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

11.4.1 Kuvaa poikkeamien havaitsemisen, reagoinnin ja forensisen valmiuden periaatteet, mukaan lukien suunnittelu, hallussapitoketju ja poikkeamiin liittyvän todistusaineiston hallinta.

11.5 NIST SP 800-53 Rev.5

11.5.1 IR-1–IR-9, AU-6, PL-2: määrittää jäsennellyt vaatimukset tietoturvapoikkeamien suunnittelulle, havaitsemiselle, analysoinnille, rajaamiselle ja käsittelylle. Tukee todistusaineiston

keräämistä ja todennettavuutta (AU-6) sekä varmistaa yhdenmukaisuuden järjestelmien tietoturva- ja tietosuunnitelmien kanssa (PL-2) forensisten tutkintojen aikana.

11.6 NIST SP 800-86

11.6.1 Antaa ohjeita forensisten prosessien integroimisesta laajempaan tietoturvapoikkeamien käsittelyn elinkaareen ja forensisen valmiuden varmistamiseen.

11.7 NIST SP 800-101 Rev.1

11.7.1 Keskittyy parhaisiin käytäntöihin digitaalisten tietovälineiden ja mobiililaitteiden todistusaineiston hankkimiseksi, säilyttämiseksi ja analysoimiseksi oikeudellisesti puolustettavalla tavalla.

11.8 EU:n GDPR (2016/679)

11.8.1 Artikla 5 – henkilötietojen käsittelyä koskevat periaatteet: soveltuu todistusaineistoon, joka sisältää henkilötietoja tai arkaluonteisia tietoja, ja varmistaa minimoinnin ja käyttötarkoitussidonnaisuuden.

11.8.2 Artiklat 33–34 – henkilötietojen tietoturvaloukkausta koskeva ilmoitus: forensinen data tukee loukkausilmoitusvelvoitteiden täyttämistä ja oikeudellisia tiedonantoprosesseja.

11.9 EU:n NIS2-direktiivi (2022/2555)

11.9.1 Artikla 23 – ilmoitusvelvollisuudet: forensinen dokumentaatio ja havainnot tukevat oikea-aikaisia ja täsmällisiä poikkeamaraportteja toimivaltaisille viranomaisille.

11.10 EU:n DORA-asetus (2022/2554)

11.10.1 Artikla 17 – ICT-poikkeamien raportointi: edellyttää yksityiskohtaisia juurisyytä ja todistusaineistoa koskevia tallenteita merkittävistä ICT-poikkeamista erityisesti finanssialalla.

11.11 COBIT 2019

11.11.1 DSS01.07 – tietoturvapoikkeamien hallinta: edellyttää poikkeamien dokumentointia ja tutkinnallista huolellisuutta.

11.11.2 DSS05.04 – tietoturvatutkintojen hallinta: korostaa digitaalisen todistusaineiston säilyttämistä sekä kurinpidollisten ja oikeudellisten toimenpiteiden tukemista.