					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P31S					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	Kohdat 6.1, 6.3, 8	Riskiperusteinen suunnittelu, parannustoimenpiteet ja operatiiviset kontrollit todistusaineiston eheyden varmistamiseksi
ISO/IEC 27002:2022	Kontrollit 5.24–5.27	Ohjaa turvallista käsittelyä, poikkeamien jälkiarviointia ja todistusaineistoon perustuvia parannuksia
ISO/IEC 27035-3:2016	Kohdat 6.3, 6.4, 7	Varmistaa digitaalisen todistusaineiston asianmukaisen suunnittelun, lainmukaisen keräämisen ja turvallisen käsittelyn sekä hallussapitoketjun dokumentoinnin
NIST SP 800-53 Rev.5	IR-07, IR-08, AU-09, AU-12, PE-18	Forensinen valmius, auditointilokien suojaus ja tehokas integrointi tietoturvapoikkeamien hallintaan
EU:n GDPR	Artiklat 33, 34	Henkilötietojen tietoturvaloukkauksiin liittyvä dokumentointi ja jäljitettävyys
EU:n NIS2-direktiivi	Artikla 23	Jäljitettävä poikkeamailmoittaminen ja todistusaineiston turvallinen käsittely
EU:n DORA-asetus	Artikla 17(1), 17(2)	Varmistaa ICT:hen liittyvien poikkeamien todistusaineiston keräämisen, säilyttämisen ja säilytysaikojen hallinnan sekä forensisen luotettavuuden ja viranomaistiedusteluihin vastaamisen
COBIT 2019	DSS05.06, DSS05.07	Luotettava lokitus ja jäsennelty todistusaineiston käsittely turvallisia ja todennettavia tutkintoja varten

1. Tarkoitus

1.1. Tämä politiikka määrittää, miten organisaatio käsittelee tietoturvapoikkeamiin, tietomurtoihin tai sisäisiin tutkintoihin liittyvää digitaalista todistusaineistoa. Politiikka varmistaa, että todistusaineisto kerätään, tallennetaan ja säilytetään oikeudellisesti kestävällä tavalla siten, että auditointivalmius säilyy, tukien sekä sisäistä päätöksentekoa että mahdollisia ulkoisia toimenpiteitä.

1.2. Politiikka mahdollistaa sen, että pk-yritykset voivat suojata lokien, tiedostojen ja järjestelmäkuvien eheyden sekä osoittaa huolellisuuden ISO/IEC 27001:n, EU:n GDPR:n ja muiden soveltuvien standardien mukaisesti.

1.3. Politiikka tukee forensista valmiutta ilman edistyneitä teknisiä resursseja tai kokoaikaista IT-tiimiä määrittämällä selkeät vastuut, menettelyt ja säilytysvaatimukset.

2. Soveltamisala

2.1. Tämä politiikka koskee:

2.1.1. Kaikkia työntekijöitä, IT-palveluntarjoajia ja ulkoisia konsultteja, jotka osallistuvat tietoturvapoikkeamien käsittelyyn, tutkintaan tai tietomurron analysointiin

2.1.2. Kaikkia yrityksen järjestelmiä, mukaan lukien kannettavat tietokoneet, mobiililaitteet, palvelimet, sähköpostitilit, SaaS-ympäristöt ja pilvitallennuspalvelut (esim. Microsoft 365, Google Workspace)

2.1.3. Kaikkia tilanteita, joissa todistusaineistoa tarvitaan sisäisiä kurinpidollisia toimenpiteitä, oikeudellista puolustettavuutta, vakuutusvaatimuksia tai viranomaisyhteydenpitoa varten

2.2. Tämä kattaa sekä toteutuneet että epäillyt tapahtumat, jotka liittyvät seuraaviin:

2.2.1. Tietovuodot

2.2.2. Sisäpiiriuhat tai väärinkäytökset

2.2.3. Tietoturvaloukkaukset (esim. haittaohjelmat, luvaton pääsy)

2.2.4. Asiakasvalitukset, jotka edellyttävät digitaalista varmennusta

2.2.5. Viranomaisen tai lainvalvontaviranomaisen tiedustelut

3. Tavoitteet

3.1. Varmistaa, että kaikki todistusaineisto kerätään ja käsitellään tavalla, joka säilyttää sen eheyden, aitouden ja hallussapitoketjun.

3.2. Estää lokien, tiedostojen tai järjestelmäkuvien tahaton muuttaminen, poistaminen tai virheellinen käsittely, kun niitä voidaan tarvita tutkinnassa.

3.3. Tarjota yhtenäinen ja todennettavissa oleva toimintatapa todistusaineiston hallintaan, joka täyttää oikeudelliset ja sääntelyyn liittyvät odotukset (esim. EU:n GDPR:n mukaiset ilmoitusvelvoitteet ja EU:n NIS2-direktiivin jäljitettävyysvaatimukset).

3.4. Määrittää selkeät roolit ja vastuut, jotta todistusaineiston nopea, turvallinen ja lainmukainen talteenotto varmistetaan tietoturvapoikkeamien aikana.

3.5. Tukea pk-yrityksille soveltuvaa forensista valmiutta minimoiden monimutkaisuus ja välttäen häiriöitä päivittäisessä toiminnassa.

4. Roolit ja vastuut

4.1. Toimitusjohtaja

4.1.1. Hyväksyy kaikki muodolliset tutkinnat, jotka edellyttävät todistusaineiston keräämistä.

4.1.2. Katselmoi ja hyväksyy poikkeamaraportit, joihin liittyy mahdollisia oikeudellisia tai kurinpidollisia toimenpiteitä.

4.1.3. Päättää, onko ulkoista oikeudellista neuvontaa hankittava tai viranomaisilmoituksia tehtävä.

4.1.4. Varmistaa, että politiikka katselmoidaan ja päivitetään säännöllisesti.

4.2. IT-palveluntarjoaja / järjestelmänvalvoja

4.2.1. Kerää ja säilyttää digitaalisen todistusaineiston turvallisia menettelyjä noudattaen.

4.2.2. Dokumentoi aikaleimat, järjestelmätiedot ja käsittelyvaiheet.

4.2.3. Suojaa kaiken kerätyn aineiston suojatussa sijainnissa.

4.2.4. Avustaa forensisen analyysin toteuttamisessa tarvittaessa.

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

9. Katselmointi- ja päivitysvaatimukset

9.1. Politiikan vuosittainen katselmointi

9.1.1. Toimitusjohtajan on katselmoitava tämä politiikka vähintään kerran 12 kuukaudessa varmistaakseen seuraavat asiat:

9.1.1.1. Yhdenmukaisuus ISO/IEC 27001:n liitteen A kontrollien kanssa

9.1.1.2. Jatkuva soveltuvuus nykyisiin digitaalisiin alustoihin ja IT-palveluihin

9.1.1.3. Lokituksen, todistusaineiston säilytyksen ja forensisen valmiuden menettelyjen riittävyys

9.2. Politiikan muutosta käynnistävät tapahtumat

9.2.1. Politiikka on lisäksi katselmoitava ja päivitettävä seuraavien jälkeen:

9.2.1.1. Mikä tahansa merkittävä poikkeama, joka edellyttää todistusaineiston keräämistä

9.2.1.2. Epäonnistunut auditointi tai viranomaispyyntö, jossa todistusaineiston eheys asetettiin kyseenalaiseksi

9.2.1.3. Uusien työkalujen tai menettelyjen käyttöönotto tietoturvapoikkeamien käsittelyä tai järjestelmien seurantaa varten

9.2.1.4. Oikeudelliset muutokset (esim. päivitetyt EU:n GDPR:ää tai EU:n NIS2-direktiiviä koskevat ohjeistukset)

9.3. Muutosten hyväksyntä ja jakelu

9.3.1. Toimitusjohtajan on katselmoitava ja hyväksyttävä kaikki muutokset

9.3.2. Päivitetty versio on jaettava seuraaville:

9.3.2.1. Tutkintoihin osallistuvat IT-palveluntarjoajat ja konsultit

9.3.2.2. Kaikki henkilöt, joilla on järjestelmänvalvontaan liittyviä vastuita

9.3.3. Päivitetty kopio on säilytettävä yrityksen politiikka-arkistossa ja jaettava auditoijille pyynnöstä

10. Liittyvät politiikat ja yhteydet

10.1. Tämä politiikka on riippuvuussuhteessa seuraaviin pk-yrityksille sovitettuihin politiikkoihin:

10.1.1. P2S – Hallinnointirooleja ja vastuita koskeva politiikka: Määrittää toimivallan poikkeamatutkintoihin, todistusaineistoa koskeviin päätöksiin sekä laki- ja sääntelyasioiden eskalointiin.

10.1.2. P4S – Pääsynhallintapolitiikka: Varmistaa, että vain valtuutetut henkilöt voivat käyttää arkaluonteisia järjestelmiä ja lokeja tutkintojen aikana.

10.1.3. P22S – Lokitus- ja valvontapolitiikka: Tuottaa forensisen todistusaineiston raakatiedot ja määrittää säilytystä, pääsynhallintaa ja lokitusta koskevat vaatimukset.

10.1.4. P30S – Tietoturvapoikkeamien hallintapolitiikka: Käynnistää tarpeen todistusaineiston keräämiselle ja määrittää operatiivisen kulun, joka johtaa forensiseen säilyttämiseen.

10.1.5. P17S – Tietosuoja- ja yksityisyydensuojapolitiikka: Varmistaa, että todistusaineistona kerättyjä henkilötietoja käsitellään lainmukaisesti EU:n GDPR:n ja siihen liittyvän sääntelyn mukaisesti.

10.2. Nämä politiikat muodostavat yhdessä perustan oikeudelliselle puolustettavuudelle, tutkinnan eheydelle ja valmiudelle osoittaa ISO/IEC 27001:2022:n mukainen vaatimustenmukaisuus auditoinneissa.

11. Viitestandardit ja viitekehykset

11.1. ISO/IEC 27001

11.1.1. Kohta 6.1 – Riskiperusteinen suunnittelu sisältää reagointivalmiuden ja todistusaineistoa koskevat menettelyt.

11.1.2. Kohta 6.3 – Tukee poikkeamista saadun todistusaineiston perusteella tehtäviä parannustoimenpiteitä.

11.1.3. Kohta 8.1 – Edellyttää operatiivisia kontrolleja todistusaineiston eheyden varmistamiseksi.

11.2. ISO/IEC 27002

11.2.1. Kontrollit 5.24–5.27 – Ohjaavat turvallista käsittelyä, poikkeamien jälkiarviointia ja todistusaineistoon perustuvia parannuksia.

11.3. ISO/IEC 27035-3

11.3.1. Kohdat 6.3, 6.4 ja 7.3 varmistavat digitaalisen todistusaineiston asianmukaisen suunnittelun, lainmukaisen keräämisen ja turvallisen käsittelyn tietoturvapoikkeamien käsittelyn aikana, mukaan lukien säilyttäminen ja hallussapitoketjun dokumentointi.

11.4. NIST SP 800-53 Rev. 5

11.4.1. IR-07, IR-08, AU-09 ja AU-12 varmistavat forensisen valmiuden, auditointilokien suojauksen ja todistusaineiston keräämisen tehokkaan integroinnin tietoturvapoikkeamien käsittelyn elinkaareen

11.5. NIST SP 800-86

11.5.1. Määrittää parhaat käytännöt digitaalisen todistusaineiston hankintaan, analysointiin ja suojaamiseen tietoturvapoikkeamien käsittelyn aikana.

11.6. EU:n GDPR

11.6.1. Artiklat 33–34 – Edellyttävät poikkeamien ja todistusaineiston dokumentointia ja jäljitettävyyttä henkilötietojen tietoturvaloukkauksista ilmoitettaessa.

11.7. EU:n NIS2-direktiivi (2022/2555)

11.7.1. Artikla 23 – Edellyttää jäljitettävää poikkeamailmoittamista ja todistusaineiston turvallista käsittelyä keskeisille ja tärkeille toimijoille.

11.8. EU:n DORA-asetus

11.8.1. Artikla 17(1) – Varmistaa, että ICT:hen liittyviin poikkeamiin liittyvä todistusaineisto kerätään ja säilytetään tavalla, joka tukee forensisia tutkimuksia.

11.8.2. Artikla 17(2) – Edellyttää, että finanssialan toimijat säilyttävät kaikki tietoturvatapahtumiin liittyvät olennaiset tiedot ja lokit forensisen luotettavuuden ja viranomaistiedustelujen vaatimusten mukaisesti.

11.9. COBIT 2019

11.9.1. DSS05.06 – Poikkeamien seuranta, havaitseminen ja raportointi: korostaa luotettavaa lokitusta tutkinnan tueksi.

11.9.2. DSS05.07 – Poikkeamien tutkiminen ja toimenpiteet: edellyttää jäsenneltyä todistusaineiston käsittelyä turvallisten ja todennettavien tutkintojen mahdollistamiseksi.