| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Lisää tähän rekisteröidyn oikeushenkilön nimi | | | | | | | |
| Asiakirjan numero:<br>P38 | | | | | Asiakirjan nimi:<br>**Suojatun viestinnän ja monivaiheisen todennuksen politiikka** | | | | | | | |
| Versio:<br>1.0 | | Voimaantulopäivä:<br>01.01.2025 | | | Asiakirjan omistaja: | | | | | | | |
| X | Politiikka | | Standardi | | Menettely | | Lomake | | Rekisteri | | Muu | |

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

| **Hyväksynnät** | | | |
|---|---|---|---|
| **Nimi** | **Tehtävänimike** | **Päivämäärä** | **Allekirjoitus** |
| | | | |
| | | | |

**Oikeudellinen huomautus (tekijänoikeudet ja käyttörajoitukset)**

(C) 2025 Clarysec LLC. All rights reserved.

Tämä asiakirja on Clarysec LLC:n immateriaalioikeudellista omaisuutta. Tämän asiakirjan mitään osaa ei saa kopioida, käyttää uudelleen, jakaa tai muokata kaupallisiin tai käyttöönottoon liittyviin tarkoituksiin ilman nimenomaista kirjallista lupaa.
Luvaton käyttö on ehdottomasti kielletty ja voi johtaa oikeudellisiin toimiin.
Lisensointia koskevissa asioissa ota yhteyttä: info@clarysec.com

Yhdenmukaisuus standardien ja sääntelyvaatimusten kanssa

| Standardi/säädös | Kohta/artikla | Kommentti |
|---|---|---|
| ISO/IEC 27001:2022 | 5.30, 5.31, 8.24 | |
| ISO/IEC 27002:2022 | 5.15, 5.17, 5.18, 8.24, 8.28 | |
| NIST SP 800-53 Rev.5 | IA-2, IA-3, IA-5, IA-8, SC-12, SC-13, SC-31 | |
| EU:n yleinen tietosuoja-asetus (GDPR) | Art. 32(1)(b) | |
| EU:n NIS2-direktiivi | Art. 21(2)(j) | |
| EU:n DORA-asetus | Art. 9(2)(d), Art. 11 | |
| COBIT 2019 | DSS05.04, DSS05.05, DSS05. | |

**1. Tarkoitus**

1.1 Määritetään vaatimukset monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisujen käytölle järjestelmien käytössä EU:n NIS2-direktiivin 21 artiklan 2 kohdan j alakohdan mukaisesti.

1.2 Määritetään suojattua puhe-, video-, teksti- ja hätäviestintää koskevat kontrollit tiedon luottamuksellisuuden ja eheyden suojaamiseksi.

**2. Soveltamisala**

2.1 Tätä politiikkaa sovelletaan kaikkiin organisaation käyttämiin todennusmekanismeihin ja viestintäjärjestelmiin (puhelut, videokokoukset, viestintäpalvelut ja hätäviestintäjärjestelmät).

2.2 Se koskee kaikkia työntekijöitä, toimeksisaajia ja muita ulkoisia osapuolia, jotka käyttävät organisaation viestintäkanavia tai sen verkko- ja tietojärjestelmiä.

**3. Tavoitteet**

3.1 Varmistetaan, että vain asianmukaisesti todennetut käyttäjät saavat pääsyn järjestelmiin, ja vähennetään luvattoman pääsyn riskiä monivaiheisella todennuksella.

3.2 Varmistetaan, että sisäinen viestintä ja hätäviestintä välitetään suojattuja menetelmiä käyttäen (esim. salattujen kanavien kautta), jotta estetään salakuuntelu ja tietojen muuttaminen.

3.3 Täytetään EU:n NIS2-direktiivin vahvaa tunnistautumista ja turvallista viestintää koskevat vaatimukset sekä vahvistetaan organisaation yleistä kyberhäiriönsietokykyä.

**4. Roolit ja vastuut**

4.1 Tietoturvajohtaja (CISO) / IT-tietoturva: määrittää ja ylläpitää monivaiheisen todennuksen mekanismit ja suojatut viestintävälineet sekä varmistaa tämän politiikan teknisen toteutuksen.

4.2 IT-järjestelmänvalvojat: ottavat monivaiheisen todennuksen käyttöön soveltuvissa järjestelmissä, konfiguroivat hyväksytyt suojatut viestintäalustat ja seuraavat vaatimustenmukaisuutta.

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

**9. Seuranta ja auditointi**

9.1 IT-tietoturvan on seurattava jatkuvasti todennuslokeja yksivaiheisten kirjautumisyritysten tai poikkeavien monivaiheisen todennuksen epäonnistumisten havaitsemiseksi. Suojattujen viestintäjärjestelmien lokeja on soveltuvin osin seurattava luvattomien käyttöyritysten tai konfiguraatiomuutosten havaitsemiseksi.

9.2 Sisäinen tarkastus arvioi vuosittain monivaiheisen todennuksen käyttöönoton noudattamista (varmistaen, että kaikki kriittiset järjestelmät edellyttävät monivaiheisen todennuksen käyttöä) ja varmentaa, että hyväksyttyjä suojattuja kanavia käytetään yksinomaan arkaluonteiseen viestintään. Havainnot raportoidaan johdolle suosituksineen.

**10. Katselmointi ja ylläpito**

10.1 Tämä politiikka katselmoidaan vähintään vuosittain sekä jokaisen merkittävän tietoturvapoikkeaman tai uuden todennukseen tai viestintään liittyvän riskin tunnistamisen yhteydessä (esim. uudet monivaiheiseen todennukseen kohdistuvat uhkavektorit tai turvattoman viestinnän käytön havaitseminen).

10.2 Päivitykset tehdään tarpeen mukaan kehittyvän teknologian huomioon ottamiseksi (esim. vahvempien jatkuvan todennuksen ratkaisujen käyttöönotto) tai päivitettyjen sääntelyohjeiden noudattamiseksi (kuten tulevat ENISAn turvallista viestintää koskevat suositukset).

**11. Liittyvät politiikat ja yhteydet**

11.1 P01 – Tietoturvapolitiikka. Määrittää organisaation laajuiset todennusta ja viestinnän suojaamista koskevat vaatimukset.

11.2 P04 – Pääsynhallintapolitiikka. Määrittää pääsynhallinnan hallintamallin, jota tämän politiikan monivaiheinen todennus tukee.

11.3 P11 – Käyttäjätilien ja käyttöoikeuksien hallintapolitiikka. Liittää monivaiheisen todennuksen etuoikeutettujen käyttöoikeuksien elinkaaren hallintaan.

11.4 P18 – Kryptografisten hallintakeinojen politiikka. Määrittää hyväksytyt kryptografiset menetelmät ja avaintenhallinnan suojattua viestintää varten.

11.5 P21 – Verkkoturvallisuuspolitiikka. Suojaa puhe-, video- ja viestintäpalveluissa käytettävät siirtokanavat.

11.6 P22 – Lokitus- ja valvontapolitiikka. Määrittää todennustapahtumien ja suojattujen kanavien käytön seurannan.

11.7 P32 – Liiketoiminnan jatkuvuus- ja katastrofipalautuspolitiikka. Varmistaa hätäviestinnän turvallisuuden kriisitilanteissa.

11.8 P08 – Tietoturvatietoisuus- ja koulutuspolitiikka. Kouluttaa käyttäjiä monivaiheisen todennuksen ja viestintäkanavien turvalliseen käyttöön.

**12. Viitteet**

12.1 NIS2-direktiivi (EU 2022/2555), 21 artiklan 2 kohta, j alakohta (monivaiheisen todennuksen ja turvallisen viestinnän käyttö)

12.2 Komission täytäntöönpanoasetus (EU) 2024/2690, liitteen kohta 11 (pääsynhallintavaatimukset, mukaan lukien monivaiheinen todennus etuoikeutetuille tileille)

12.3 ISO/IEC 27001:2022 ja ISO/IEC 27002:2022