					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P22					Asiakirjan nimi: **Lokitus- ja valvontapolitiikka**							
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**

1. Tarkoitus

1.1 Tämän politiikan tarkoituksena on määrittää selkeät ja toimeenpantavat vaatimukset sellaisten lokien tuottamiselle, suojaamiselle, katselmoinnille ja analysoinnille, joihin tallentuu keskeisiä järjestelmä- ja tietoturvatapahtumia koko organisaation IT-ympäristössä.

1.2 Lokitus ja valvonta ovat kriittisiä poikkeamien havaitsemisen, uhkiin reagoinnin, forensisten tutkintojen, auditointivalmiuden ja lakisääteisen vaatimustenmukaisuuden kannalta. Tämä politiikka varmistaa, että kaikki järjestelmien tuottamat tapahtumat kirjataan asianmukaisesti, säilytetään ja korreloidaan aikasynkronoidusti.

1.3 Tämä politiikka on olennainen ISO/IEC 27001 -standardin lausekkeen 8.1 sekä liitteen A kontrollien 8.15 (Lokitus), 8.16 (Valvonta) ja 8.17 (Kellon synkronointi) tukemiseksi, ja se kohdistuu suoraan GDPR:n, NIS2-direktiivin, DORA-asetuksen ja COBIT 2019:n sääntelyvelvoitteisiin.

2. Soveltamisala

2.1 Tätä politiikkaa sovelletaan kaikkiin järjestelmiin, palveluihin ja ympäristöihin, jotka tallentavat, käsittelevät tai siirtävät tietoja ja jotka kuuluvat tietoturvallisuuden hallintajärjestelmän (ISMS) piiriin, mukaan lukien:

2.1.1 paikallinen infrastruktuuri, pilvipalvelut (esim. IaaS, PaaS, SaaS) ja hybridiympäristöt

2.1.2 käyttöjärjestelmät, tietokannat, sovellukset ja verkkolaitteet

2.1.3 tietoturvajärjestelmät, kuten SIEM-järjestelmät, palomuurit, päätelaitteiden havainnointi- ja reagointialustat (EDR), VPN-keskittimet ja identiteetin tarjoajat

2.2 Seuraavat sidosryhmät kuuluvat soveltamisalaan:

2.2.1 sisäiset käyttäjät, joilla on järjestelmä- tai ylläpitäjäoikeuksia

2.2.2 infrastruktuuri- ja IT-operaatioiden henkilöstö

2.2.3 tietoturvavalvomo (SOC) ja uhkien havaitsemiseen osallistuvat tiimit

2.2.4 ohjelmistokehittäjät ja sovellusomistajat

2.2.5 kolmannen osapuolen palveluntarjoajat, jotka hallinnoivat lokeja tuottavia järjestelmiä

3. Tavoitteet

3.1 Varmistaa, että kaikki kriittiset järjestelmät tuottavat tietoturvatapahtumalokeja ja järjestelmätoiminnan tallenteita, joita säilytetään sääntely-, laki- ja sopimusvaatimusten mukaisesti.

3.2 Määrittää vähimmäistapahtumatyypit ja lokisisältö, joita tarvitaan luvattoman toiminnan havaitsemiseen, käyttäjätoimien jäljitettävyyteen ja forensisten tutkintojen tukemiseen.

3.3 Toteuttaa suojatoimet, joilla estetään lokien peukalointi, luvaton poistaminen tai hallitsematon pääsy lokitietoihin.

3.4 Määrittää keskitetyn lokituksen ja hälytysjärjestelmät (esim. SIEM), joilla epäilyttävä toiminta kootaan, korreloidaan ja eskaloidaan lähes reaaliajassa.

3.5 Varmistaa järjestelmäkellojen synkronointi, jotta järjestelmien välinen korrelaatio ja poikkeama-analyysi ovat tarkkoja.

3.6 Mahdollistaa jatkuva parantaminen ja vaatimustenmukaisuus integroimalla lokien valvonta auditointi-, riski- ja poikkeamienhallintaprosesseihin.

4. Roolit ja vastuut

4.1 tietoturvajohtaja (CISO)

4.1.1 Omistaa tämän politiikan ja varmistaa, että se on yhdenmukainen organisaation riskitason, auditointivaatimusten ja ISMS-velvoitteiden kanssa.

4.1.2 Hyväksyy lokituksen soveltamisalan sääntelyn alaisille tai korkean riskin järjestelmille ja valvoo vaatimustenmukaisuusraportointia.

4.2 tietoturvavalvomon (SOC) päällikkö

4.2.1 Vastaa keskitettyjen lokienhallinta-alustojen (esim. SIEM) käytöstä ja ylläpidosta.

4.2.2 Määrittää lokien koontisäännöt, hälytysrajat sekä poikkeamien luokittelu- ja priorisointieskalointipolut.

4.2.3 Katselmoi päivittäiset raportit ja varmistaa, että poikkeamat analysoidaan, dokumentoidaan ja eskaloidaan tarvittaessa.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Tämä politiikka on katselmoitava vuosittain tai aikaisemmin seuraavissa tilanteissa:

9.1.1 merkittävät muutokset järjestelmäarkkitehtuurissa tai lokitusinfrastruktuurissa (esim. SIEM-migraatio)

9.1.2 muutokset lokitusta koskevissa sääntelyvaatimuksissa (esim. NIS2-direktiivin tai DORA-asetuksen lokitusvelvoitteet)

9.1.3 auditointihavainnot tai poikkeamien jälkiarvioinnit

9.1.4 esiin nousevat uhat, jotka edellyttävät tehostettua valvontaa (esim. sisäiset uhat, toimitusketjun vaarantuminen)

9.2 Katselmointiprosessia johtaa tietoturvavalvomon (SOC) päällikkö yhteistyössä tietoturvajohtajan (CISO), riskienhallinnan, vaatimustenmukaisuustoiminnon ja IT-infrastruktuuritiimien kanssa.

9.3 Hyväksytyt muutokset on pidettävä versiohallittuina ISMS:n dokumenttienhallintarekisterissä, ja niistä on tiedotettava:

9.3.1 kaikille sidosryhmille, jotka vastaavat lokitusjärjestelmien ylläpidosta

9.3.2 sovellusomistajille ja järjestelmäomistajille

9.3.3 kolmannen osapuolen palveluntarjoajille, joilla on telemetriaan tai SIEM-integraatioon liittyviä velvollisuuksia

9.4 Kaikki korvatut versiot on arkistoitava turvallisesti, ja pääsy niihin on rajattava valtuutetuille ISMS:stä vastaaville henkilöille auditointi- ja oikeudellisia tarkoituksia varten.

10. Liittyvät politiikat ja yhteydet

10.1 P1 – Tietoturvapolitiikka. Määrittää perustason sitoumuksen järjestelmien ja tietojen suojaamiseen, jonka puitteissa lokitus ja valvonta toimivat keskeisinä havaitsevina kontrolleina ja reagoinnin mahdollistajina.

10.2 P4 – Pääsynhallintapolitiikka. Varmistaa, että etuoikeutettu pääsy, käyttäjäkirjautumiset ja valtuutustapahtumat tallentuvat lokeihin ja että niitä valvotaan väärinkäytön tai poikkeavan toiminnan havaitsemiseksi.

10.3 P5 – Muutoksenhallintapolitiikka. Edellyttää järjestelmämuutosten, korjauspäivitysten käyttöönottojen ja konfiguraatiopäivitysten lokitusta, kun ne voivat aiheuttaa riskiä tai johtaa luvattomiin muutoksiin.

10.4 P21 – Verkkoturvallisuuspolitiikka. Edellyttää verkkotason lokitusta (esim. palomuurilokit, IDS/IPS-hälytykset, VPN-toiminta) ja integraatiota SIEM-järjestelmään verkkoliikenteen poikkeamien ja rajasuojauksen näkyvyyden varmistamiseksi.

10.5 P23 – Kellon synkronointipolitiikka. Edellyttää kellonaikojen yhdenmukaisuutta eri järjestelmissä, mikä on olennaista luotettavan lokituksen ja eri ympäristöissä syntyvien tietoturvatapahtumien korrelaation kannalta.

10.6 P30 – Tietoturvapoikkeamien hallintapolitiikka. Perustuu lokitietoihin ja hälytysmekanismeihin tietoturvapoikkeamien tunnistamisessa, tutkinnassa ja käsittelyssä sekä forensisten artefaktien säilyttämisessä poikkeaman jälkiarviointia varten.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Lauseke 8.1 – Operatiivinen suunnittelu ja ohjaus: edellyttää kontrolleja toimintojen valvontaan sekä suojausta luvatonta pääsyä ja järjestelmien väärinkäyttöä vastaan.

11.2 ISO/IEC 27002:2022 – Kontrollit 8.15, 8.16, 8.17

11.2.1 Määrittää yksityiskohtaiset lokitusvaatimukset, mukaan lukien mitkä tapahtumat on tallennettava, miten lokit suojataan ja analysoidaan sekä miten aikaleimojen luotettavuus varmistetaan eri järjestelmissä.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-2–AU-12: kattaa tapahtumien valinnan, lokituksen, suojaamisen, auditointikatselmoinnin, auditointivirheisiin reagoinnin ja auditointitallenteiden säilyttämisen.

11.3.2 SI-4 – Järjestelmän valvonta: edellyttää aktiivista järjestelmien valvontaa poikkeavaan toimintaan perustuvilla hälytyksillä.

11.3.3 SC-45 – Järjestelmäajan synkronointi: vahvistaa ajan tarkkuuden merkitystä tapahtumien jäljitettävyyden ja poikkeamien korrelaation kannalta.

11.4 EU:n GDPR (2016/679)

11.4.1 Artikla 32 – Käsittelyn turvallisuus: edellyttää teknisiä kontrolleja, kuten lokitusta ja valvontaa, turvallisuuden ja osoitusvelvollisuuden varmistamiseksi erityisesti henkilötietoihin kohdistuvan pääsyn osalta.

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

11.5.1 Artikla 21(2)(e): edellyttää tapahtumien lokitusta ja valvontajärjestelmiä tietoturvapoikkeamien nopeaa havaitsemista ja niihin reagointia varten.

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

11.6.1 Artikla 9 – ICT-riskien hallinta: edellyttää mekanismeja poikkeavan toiminnan havaitsemiseen, poikkeamien kirjaamiseen lokiin ja forensisten tietojen säilyttämiseen.

11.6.2 Artikla 11 – ICT-liiketoiminnan jatkuvuussuunnitelmien testaus: korostaa valvonnan jatkuvuutta ja lokien saatavuuden validointia toiminnallisten häiriöiden aikana.

11.7 COBIT 2019

11.7.1 DSS01.05 – Tietoturvalokien hallinta: edellyttää lokituskyvykkyyksien toteutusta kaikessa kriittisessä infrastruktuurissa.

11.7.2 DSS05.04 – Tietoturvatapahtumien valvonta: edellyttää lokien reaaliaikaista valvontaa ja analysointia tapahtumien havaitsemiseksi ja niihin reagoimiseksi.

11.7.3 MEA03 – Vaatimustenmukaisuuden seuranta, arviointi ja tarkastelu: edellyttää lokituskäytäntöjen säännöllistä katselmointia ja yhdenmukaisuutta kontrollitavoitteiden kanssa.