					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P22S					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**

Yhdenmukaisuus standardien ja sääntelyvaatimusten kanssa

Standardi/sääntely	Lauseke/artikla	Kommentti
ISO/IEC 27001:2022	Lauseke 8	Operatiiviset kontrollit, mukaan lukien lokitus
ISO/IEC 27002:2022	Kontrollit 8.15, 8.16, 8.17	Tapahtumalokitus, lokien suojaus ja valvonta
NIST SP 800-53 Rev.5	AU-2–AU-12, SI-4	Auditointilokien sisältö ja katselmointi, säilytys, poikkeamien havaitseminen ja hälytykset
EU:n GDPR	Artiklat 5(1)(f), 32, 33	Tietojen luottamuksellisuus ja eheys, tekniset toimenpiteet sekä tietoturvaloukkauksista ilmoittaminen
EU:n NIS2-direktiivi	Artiklat 21(2)(d), 23	Poikkeamien havaitsemista tukevat lokitusmekanismit ja poikkeamista ilmoittaminen 24 tunnin kuluessa
EU:n DORA-asetus	Artiklat 10, 15	Operatiivinen häiriönsietokyky, palveluntarjoajien valvonta ja lokitus
COBIT 2019	DSS01.03, DSS05.02	Toiminnan jäljitettävyys sekä suojaaminen lokituksen ja valvonnan avulla

1. Tarkoitus

1.1 Tällä politiikalla määritetään pakolliset lokitus- ja valvontakontrollit organisaation IT-järjestelmien turvallisuuden, osoitusvelvollisuuden ja toiminnallisen eheyden varmistamiseksi.

1.2 Tässä politiikassa määritetään lokitettavat tapahtumatyypit, lokien säilytys, lokien katselmointi sekä henkilöstön ja palveluntarjoajien vastuut.

1.3 Lokitus ja valvonta tukevat uhkien havaitsemista, vaatimustenmukaisuutta, poikkeamien käsittelyä ja forensista analyysiä.

1.4 Tämän politiikan avulla organisaatio täyttää ISO/IEC 27001 -standardin operatiivisia kontrolleja koskevat vaatimukset sekä ylläpitää auditointivalmiutta, asiakkaiden luottamusta ja GDPR:n, NIS2:n ja DORA:n noudattamista.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia organisaation järjestelmiä ja käyttäjiä, mukaan lukien:

2.1.1 työasemat, kannettavat tietokoneet, palvelimet, palomuurit, kytkimet, reitittimet ja langattomat tukiasemat

2.1.2 liiketoiminnassa käytettävät pilvipalvelut (esim. sähköposti, tiedostojen tallennus, varmuuskopiointi ja yhteistyövälineet)

2.1.3 virustorjuntaohjelmistojen, sovellusten, käyttöjärjestelmien ja verkkolaitteiden lokitustoiminnot

2.1.4 kaikki työntekijät, sopimuskumppanit ja hallinnoidut palveluntarjoajat (MSP), jotka käyttävät tai ylläpitävät järjestelmiä

2.1.5 kaikki sijainnit, joissa yrityksen IT-järjestelmiä käytetään, mukaan lukien etätyö-, hybridityö- ja BYOD-ympäristöt

2.2 Tämä politiikka koskee myös kolmannen osapuolen palvelujen tuottamia lokeja silloin, kun organisaatiolla on hallinnollinen pääsy niihin tai sopimukseen perustuvat tarkastusoikeudet.

3. Tavoitteet

3.1 Varmistaa järjestelmätoiminnan lokitus, mukaan lukien todennus, konfiguraatiomuutokset, pääsy arkaluonteisiin tietoihin ja tietoturvahälytykset.

3.2 Ylläpitää turvallisia ja tarkkoja lokeja politiikkarikkomusten, järjestelmävirheiden ja luvattomien toimien havaitsemiseksi.

3.3 Mahdollistaa lokien nopea katselmointi poikkeamien, tutkintojen ja auditointien aikana.

3.4 Tukea aikasynkronointia lokitietojen eheyden ja keskinäisen korreloinnin varmistamiseksi.

3.5 Suojata lokit peukaloinnilta, häviämiseltä ja ennenaikaiselta poistamiselta.

3.6 Täyttää järjestelmien osoitusvelvollisuutta, jäljitettävyyttä ja tietoturvaloukkausten käsittelyä koskevat lakisääteiset ja sääntelyyn perustuvat velvoitteet.

4. Roolit ja vastuut

4.1 Toimitusjohtaja

4.1.1 hyväksyy tämän politiikan ja varmistaa sen toimeenpanon kaikissa liiketoimintajärjestelmissä

4.1.2 katselmoi IT-toiminnon tai tietosuojatoiminnon raportoimat korkean vakavuustason hälytykset ja merkittävät auditointihavainnot

4.1.3 hyväksyy poikkeukset tilanteissa, joissa lokitusta tai säilytystä ei voida teknisesti toteuttaa

4.2 IT-palveluntarjoaja / sisäinen IT-vastaava

4.2.1 toteuttaa ja konfiguroi lokituksen käyttöjärjestelmissä, verkkolaitteissa, virustorjuntatyökaluissa ja keskeisissä sovelluksissa

4.2.2 varmistaa, että lokit säilytetään, varmuuskopioidaan ja suojataan muutoksilta

4.2.3 katselmoi lokit säännöllisesti ja tutkii epäilyttävän tai luvattoman toiminnan

4.2.4 ylläpitää hälytysjärjestelmiä, jotka tunnistavat poikkeavan käyttäytymisen tai tunkeutumisen indikaattorit

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Vuosittainen katselmointi

9.1.1 Toimitusjohtajan on katselmoitava tämä politiikka vähintään vuosittain IT-palveluntarjoajan ja tietosuojakoordinaattorin tukemana.

9.2 Katselmoinnin käynnistävät tekijät

9.2.1 Suunnittelemattomia katselmointeja on tehtävä seuraavien tapahtumien johdosta:

9.2.1.1 lokitukseen liittyvät havainnot sisäisissä tai ulkoisissa auditoinneissa

9.2.1.2 tietoturvapoikkeamat, joissa lokit puuttuivat, olivat vioittuneet tai riittämättömät

9.2.1.3 olennaiset muutokset IT-infrastruktuurissa (esim. siirtyminen pilvipohjaisiin lokitusalustoihin)

9.2.1.4 lakisääteisten tai sääntelyyn perustuvien velvoitteiden muutokset (esim. GDPR, NIS2, DORA)

9.3 Versionhallinta

9.3.1 Kaikki tämän politiikan muutokset on kirjattava versionumeron, päivämäärän ja muutosten yhteenvedon kanssa

9.3.2 Aiemmat versiot on arkistoitava ja säilytettävä vähintään 3 vuotta

9.3.3 Päivitetyt politiikat on viestittävä niille sidosryhmille, joita muutokset koskevat, erityisesti henkilöille, joilla on järjestelmätason käyttöoikeudet

10. Liittyvät politiikat ja yhteydet

10.1 Tämä politiikka tukee suoraan seuraavia pk-yrityksen tietoturvapolitiikkoja, ja ne tukevat tätä politiikkaa:

10.1.1 P17S – Tietosuoja- ja yksityisyydensuojapolitiikka: varmistaa, että henkilötietoja sisältäviä lokitietoja hallitaan eheyden, säilytyksen ja pääsyn suojaustoimenpiteiden osalta GDPR:n vaatimusten mukaisesti.

10.1.2 P21S – Verkkoturvallisuuspolitiikka: muodostaa perustan palomuureihin, langattomaan käyttöön, VPN-yhteyksiin ja segmentoinnin valvontaan liittyvien lokien keräämiselle.

10.1.3 P24S – Turvallisen kehittämisen politiikka: varmistaa, että sovelluslokit (esim. kirjautumisyritykset, virheet ja poikkeukset) sisällytetään ohjelmistojen suunnitteluun ja käyttöön.

10.1.4 P30S – Tietoturvapoikkeamien hallintapolitiikka: perustuu tarkkoihin ja kattaviin lokitietoihin tietoturvatapahtumien havaitsemiseksi, analysoimiseksi ja käsittelemiseksi.

10.1.5 P23S – Aikasynkronointipolitiikka: varmistaa yhdenmukaiset ja jäljitettävät aikaleimat kaikissa järjestelmissä, jotta lokit voidaan korreloida tutkintojen aikana.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Lauseke 8.1 – Edellyttää operatiivisten kontrollien toteuttamista tietoturvariskien lieventämiseksi, mukaan lukien lokitus.

11.2 ISO/IEC 27002

11.2.1 Kontrolli 8.15 – Edellyttää tapahtumalokitusta poikkeamien havaitsemisen ja osoitusvelvollisuuden tukemiseksi.

11.2.2 Kontrolli 8.16 – Edellyttää lokien suojaamista peukaloinnilta ja luvattomalta käytöltä.

11.2.3 Kontrolli 8.17 – Edellyttää järjestelmien valvontaa poikkeavan toiminnan havaitsemiseksi ja valvontakontrollien tehokkuuden varmistamiseksi.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2–AU-12 – Kattaa auditointilokien sisällön, katselmoinnin, säilytyksen ja automatisoidut hälytykset.

11.3.2 SI-4 – Edellyttää järjestelmäpoikkeamien havaitsemista ja epäilyttävien tapahtumien raportointia.

11.4 EU:n GDPR

11.4.1 Artikla 5(1)(f) – Edellyttää henkilötietojen eheyttä ja luottamuksellisuutta, mukaan lukien pääsyn lokitus.

11.4.2 Artikla 32 – Velvoittaa toteuttamaan teknisiä ja organisatorisia toimenpiteitä turvallisuuden varmistamiseksi, mukaan lukien lokitus ja valvonta.

11.4.3 Artikla 33 – Edellyttää oikea-aikaista tietoturvaloukkauksista ilmoittamista, jota tukevat juurisyyanalyysin mahdollistavat lokit.

11.5 EU:n NIS2-direktiivi

11.5.1 Artikla 21(2)(d) – Edellyttää lokitusmekanismeja, jotka havaitsevat poikkeamia ja tukevat poikkeamien tutkintaa.

11.5.2 Artikla 23 – Velvoittaa ilmoittamaan poikkeamista 24 tunnin kuluessa, mikä edellyttää tarkkoja ja ajantasaisia lokitietoja.

11.6 EU:n DORA-asetus

11.6.1 Artikla 10 – Edellyttää digitaalista toiminnallista häiriönsietokykyä, mukaan lukien ICT:hen liittyvien poikkeamien jäljitettävyys lokituksen avulla.

11.6.2 Artikla 15 – Velvoittaa valvomaan palveluntarjoajia, mukaan lukien oikeudet lokien saantiin ja katselmointiin.

11.7 COBIT 2019

11.7.1 DSS01.03 – Edellyttää järjestelmätoiminnan jäljitettävyyttä lokituksen ja valvonnan avulla.

11.7.2 DSS05.02 – Käsittelee lokitusta keskeisenä kontrollina haittaohjelmilta ja muulta luvattomalta toiminnalta suojautumisessa.