					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P39					Asiakirjan nimi: **Haavoittuvuuksien koordinoidun julkistamisen 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	6.1.3	
ISO/IEC 27002:2022	5.7, 8.8, 8.9, 8.28, 8.29	
NIST SP 800-53 Rev.5	RA-5, SI-2, PM-15, CA-8, SR-6	
EU:n GDPR	Art. 32(1)(d)	
EU:n NIS2-direktiivi	Art. 21(2)(e)	
EU:n DORA-asetus	Art. 11(1)(d)	
COBIT 2019	DSS05.01, DSS05.07, BAI09.02, MEA02.01	

1. Tarkoitus

1.1 Määrittää muodollinen prosessi organisaation järjestelmiin tai palveluihin vaikuttavia haavoittuvuuksia koskevien tietojen vastaanottamiselle, käsittelylle ja julkistamiselle EU:n NIS2-direktiivin 21 artiklan 2 kohdan e alakohdan edellyttämällä tavalla.

1.2 Kannustaa ulkoisia tietoturvatutkijoita, kumppaneita ja käyttäjiä ilmoittamaan haavoittuvuuksista vastuullisesti (Coordinated Vulnerability Disclosure, CVD) sekä määrittää, miten organisaatio viestii haavoittuvuuksia koskevista tiedoista sidosryhmille.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia organisaation omistamia tai käyttämiä verkko- ja tietojärjestelmiä sekä niissä tunnistettuja haavoittuvuuksia.

2.2 Se kattaa sisäiset tiimit (tietoturva, IT ja kehitys) sekä kaikki haavoittuvuuksista ilmoittavat ulkoiset osapuolet (esimerkiksi tutkijat, asiakkaat ja toimittajat). Politiikka ohjaa myös viestintää tuotetoimittajien tai palveluntarjoajien kanssa, jos haavoittuvuus liittyy niiden komponentteihin.

3. Tavoitteet

3.1 Tunnistaa ja korjata tietoturvahaavoittuvuudet oikea-aikaisesti hyödyntämällä sekä sisäisiä arviointeja että ulkoisia ilmoituksia.

3.2 Antaa ulkoisille ilmoittajille selkeät ohjeet haavoittuvuustietojen turvalliseen ja lainmukaiseen toimittamiseen sekä organisaatiolle tehokkaaseen reagointiin ja korjaamiseen.

3.3 Varmistaa yhdenmukaisuus EU:n NIS2-direktiivin vaatimusten ja toimialan parhaiden käytäntöjen (ISO/IEC 29147 ja ISO/IEC 30111) kanssa haavoittuvuuksien koordinoidussa julkistamisessa sekä parantaa koko ekosysteemin turvallisuutta.

4. Roolit ja vastuut

4.1 Haavoittuvuuksiin reagointitiimi (VRT): Nimetty tiimi, jota johtaa tietoturvajohtaja (CISO) tai haavoittuvuuksien hallinnasta vastaava henkilö. Tiimi vastaanottaa ja luokittelee haavoittuvuusilmoitukset, arvioi riskit ja vaikutukset sekä koordinoi korjaavat toimenpiteet ja julkistamisen.

4.2 IT- ja kehitystiimit: Tekevät yhteistyötä VRT:n kanssa ilmoitettujen haavoittuvuuksien validoinnissa, korjauspäivitysten tai lieventävien toimenpiteiden kehittämisessä ja testaamisessa sekä korjausten käyttöönotossa. Toimittavat tarvittaessa tekniset tiedot tiedotteita varten.

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

9. Seuranta ja auditointi

9.1 VRT ylläpitää haavoittuvuuksien julkistuslokia, jossa seurataan jokaista ilmoitusta vastaanotosta sulkemiseen saakka. Loki katselmoidaan kuukausittain, jotta avoimien asioiden käsittely etenee ajallaan. Myöhässä olevat asiat eskaloidaan.

9.2 Sisäinen tarkastus tai riippumaton tietoturva-arvioija arvioi vuosittain haavoittuvuuksien käsittelyprosessin tehokkuuden tarkastamalla esimerkiksi, että otos haavoittuvuustapauksista on käsitelty tämän politiikan mukaisesti (vastaanotto kuitattu, korjaus toteutettu ja julkistaminen tehty ajallaan). Samalla varmennetaan, että julkinen ilmoituskanava toimii (esimerkiksi testisähköpostit vastaanotetaan ja käsitellään).

9.3 Haavoittuvuuksia koskevat mittarit (määrä vakavuusluokittain, korjausajat jne.) kootaan neljännesvuosittain ja esitetään kyberturvallisuuden hallintakomitealle riskienarvioinnin päivitysten tueksi.

10. Katselmointi ja ylläpito

10.1 Tämä politiikka katselmoidaan vähintään vuosittain. Lisäksi mikä tahansa merkittävä muutos IT-ympäristössämme (esimerkiksi uuden internetiin avautuvan palvelun käyttöönotto) tai asiaankuuluva sääntelymuutos (esimerkiksi uusi EU-sääntely tuotteiden haavoittuvuuksien julkistamisesta) käynnistää ylimääräisen katselmoinnin.

10.2 Politiikan päivityksissä otetaan huomioon ulkoisten ilmoittajien palaute ja sisäisten jälkiarviointien opit. Merkittävät muutokset hyväksyy tietoturvajohtaja (CISO), ja niistä viestitään kaikille työntekijöille sekä ne julkaistaan verkkopalvelussa tietoturvapolitiikkojen tietovarastossa läpinäkyvyyden varmistamiseksi.

11. Liittyvät politiikat ja yhteydet

11.1 P01 – Tietoturvapolitiikka. Johdon toimeksianto haavoittuvuuksien käsittelylle ja julkistamiselle.

11.2 P19 – Haavoittuvuuksien ja korjauspäivitysten hallintapolitiikka. Sisäinen korjausprosessi, joka liittyy CVD-ilmoitusten vastaanottoon.

11.3 P24 – Turvallisen kehittämisen politiikka. Tukee korjausten toteutusta ja ohjelmistokehityksen elinkaaren vahvistamista ilmoitettujen havaintojen perusteella.

11.4 P25 – Sovellusturvallisuusvaatimusten politiikka. Varmistaa, että tuotteissa on julkistamisvalmiutta tukevat tietoturvavaatimukset.

11.5 P30 – Tietoturvapoikkeamien hallintapolitiikka. Kattaa julkistettujen haavoittuvuuksien aktiivisen hyväksikäytön käsittelyn.

11.6 P31 – Todisteiden keräämisen ja digitaalisen forensiikan politiikka. Säilyttää ilmoitettuihin tai hyväksikäytettyihin puutteisiin liittyvät artefaktit.

11.7 P26 – Kolmansien osapuolten ja toimittajaturvallisuuden politiikka. Koordinoi toimittajien komponentteihin liittyviä julkistamisia.

11.8 P37 – Laki- ja sääntelyvaatimustenmukaisuuden politiikka. Ohjaa ilmoittamista, safe harbor -muotoiluja ja julkaisemista.

12. Viitteet

12.1 NIS2-direktiivi (EU 2022/2555), 21 artiklan 2 kohdan e alakohta (kehittämisen turvallisuus sekä haavoittuvuuksien käsittely ja julkistaminen)

12.2 Komission täytäntöönpanoasetus (EU) 2024/2690, liitteen kohta 6.10 (tekniset vaatimukset haavoittuvuuksien käsittely- ja julkistamisprosesseille)

12.3 ENISAn tekninen ohjeistus kyberturvallisuusriskien hallintatoimenpiteistä – osio haavoittuvuuksien käsittelystä ja julkistamisesta

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:2022 (kontrolli A.5.7 uhkatiedustelusta ja haavoittuvuuksien julkistamisesta; kontrolli A.8.28 turvallisesta kehittämisestä)

12.5 ISO/IEC 29147:2018 (ohjeet haavoittuvuuksien julkistamisesta) ja ISO/IEC 30111:2019 (ohjeet haavoittuvuuksien käsittelyprosesseista)