					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P19					Asiakirjan nimi: **Haavoittuvuuksien ja korjauspäivitysten hallintapolitiikka**							
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	Teknisten haavoittuvuuksien järjestelmällinen käsittely; tietoturvakontrollien jatkuva vaikuttavuus.
ISO/IEC 27002:2022	Kontrollit 8.8, 8.9, 5	Toteutusohjeet paikkaamiseen, haavoittuvuusskannaukseen, ohjelmistojen eheyteen, turvalliseen konfigurointiin ja omaisuusluetteloihin.
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2, CM-6	Tiheä skannaus, puutteiden korjaaminen ja konfiguraationhallinta on otettu käyttöön.
EU:n GDPR	Artikla 32, johdanto-osan kappale 49	Tekniset toimenpiteet viipymättömään paikkaamiseen, haavoittuvuuksien käsittelyyn ja tietoturvan jatkuvuuden varmistamiseen.
EU:n NIS2-direktiivi	Artikla 21(2)(d)	Haavoittuvuuksien havaitseminen, niihin reagointi ja niiden lieventäminen korkean kyberhygienian tason varmistamiseksi.
EU:n DORA-asetus	Artiklat 8, 10(2)(f)	ICT-haavoittuvuuksien oikea-aikainen korjaaminen; jatkuvat uhkalähtöiset arvioinnit.
COBIT 2019	DSS05.02, DSS01.03, MEA	Teknisten heikkouksien skannaus, seuranta ja lieventäminen; hyväksikäytön seuranta; vaikuttavuuden auditointi, mukaan lukien korjauspäivitysten tila.

1. Tarkoitus

1.1 Tämä politiikka määrittää organisaation pakolliset vaatimukset kaikkien tietoturvallisuuden hallintajärjestelmän (ISMS) soveltamisalaan kuuluvien tietojärjestelmien ja omaisuuserien teknisten haavoittuvuuksien ja ohjelmistopuutteiden tunnistamiselle, luokittelulle, korjaamiselle ja seurannalle.

1.2 Politiikka varmistaa, että kaikki tunnetut haavoittuvuudet arvioidaan ja käsitellään riskiperusteisesti sekä oikea-aikaisesti koordinoidun paikkaamisen, konfiguraatiomuutosten tai korvaavien kontrollien avulla liiketoiminnan tarpeiden ja vaatimustenmukaisuusvelvoitteiden mukaisesti.

1.3 Tämä politiikka tukee ISO/IEC 27001:n liitteen A kontrollin 8.8 ja ISO/IEC 27002:n ohjeistuksen noudattamista sekä huomioi DORA-asetuksen 8 artiklan, NIS2-direktiivin 21 artiklan, EU:n GDPR:n 32 artiklan sekä COBIT 2019:n DSS- ja APO-osa-alueiden vaatimukset.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia tietoturvallisuuden hallintajärjestelmän hallinnan piiriin kuuluvia tietojärjestelmiä, omaisuuseriä ja ympäristöjä, joissa tietoja säilytetään, käsitellään tai siirretään, mukaan lukien:

2.1.1 käyttöjärjestelmät, sovellukset, verkkolaitteet, laiteohjelmistot, pilvialustat, ohjelmointirajapinnat ja kolmansien osapuolten ohjelmistot.

2.1.2 kehitys-, testaus-, tuotanto-, varmuuskopiointi- ja katastrofipalautusympäristöjen järjestelmät.

2.1.3 päätelaitteet, palvelimet, IoT-laitteet, virtualisointi-infrastruktuuri ja kontit.

2.2 Tämä politiikka sitoo seuraavia tahoja:

2.2.1 Sisäinen henkilöstö: IT-järjestelmänvalvojat, järjestelmäinsinöörit, sovelluskehittäjät, tietoturva-analyytikot ja infrastruktuuritiimit.

2.2.2 Ulkoiset osapuolet: urakoitsijat, hallinnoidut palveluntarjoajat (MSP), ohjelmistotoimittajat ja järjestelmäintegraattorit, joilla on teknisiä vastuita soveltamisalaan kuuluvista omaisuuseristä.

2.3 Politiikka kattaa koko haavoittuvuuksien ja korjauspäivitysten elinkaaren, mukaan lukien:

2.3.1 skannaus ja havaitseminen

2.3.2 riskiluokittelu ja priorisointi

2.3.3 korjauspäivitysten hankinta, testaus, käyttöönotto ja palautus

2.3.4 poikkeusten käsittely ja korvaavien kontrollien suunnittelu

2.3.5 lokitus, raportointi ja auditointijäljen jäljitettävyys

3. Tavoitteet

3.1 Varmistaa, että kaikki tunnetut haavoittuvuudet tunnistetaan, arvioidaan ja korjataan tavalla, joka minimoi riskialtistuksen ja tukee operatiivisia prioriteetteja.

3.2 Määrittää yhdenmukaiset, koko organisaation kattavat menettelyt haavoittuvuusskannaukselle, vakavuusluokittelulle (esim. CVSS) ja korjauspäivitysten hallinnalle, mukaan lukien hätätilanteiden käsittely ja palautussuunnittelu.

3.3 Mahdollistaa turvallinen konfiguraationhallinta yhdenmukaistamalla koventamisen perustasot, muutoksenhallintakäytännöt ja reaaliaikaisen uhkatiedustelun.

3.4 Tuottaa mitattavaa vaatimustenmukaisuutta sääntelyyn ja standardeihin perustuvien kontrollien osalta, jotka liittyvät järjestelmien eheyteen, korjauspäivityshygieniaan ja puutteiden oikea-aikaiseen korjaamiseen.

3.5 Määrittää vastuut ja tilivelvollisuuden eri rooleille koko haavoittuvuuksien hallinnan elinkaaren ajalle siten, että kaikki sidosryhmät toimivat määritettyjen palvelutasosopimusten mukaisesti ja raportoivat kontrollien mittarit.

3.6 Tukea auditointivalmiutta ja parantaa häiriönsietokykyä esiin nousevia uhkia vastaan, mukaan lukien nollapäivähaavoittuvuudet, aktiiviset hyväksikäyttöketjut ja merkittävät toimittajailmoitukset.

4. Roolit ja vastuut

4.1 Tietoturvajohtaja (CISO)

4.1.1 Omistaa politiikan ja varmistaa sen integroinnin tietoturvallisuuden hallintajärjestelmään (ISMS).

4.1.2 Määrittää organisaation riskinsietotason ja varmistaa yhdenmukaisuuden sääntely- ja kontrollivaatimusten kanssa.

4.2 Haavoittuvuuksien hallinnasta vastaava henkilö / tietoturvavalvomon päällikkö

4.2.1 Vastaa haavoittuvuuksien ja korjauspäivitysten hallinnan päästä päähän -toiminnoista.

4.2.2 Koordinoi skannausaikatauluja, priorisointimalleja ja korjaamisen määräaikoja.

4.2.3 Ylläpitää haavoittuvuusrekisteriä ja osallistuu korvaavien kontrollien arviointiin.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Tämä politiikka on katselmoitava vähintään vuosittain tai seuraavissa tilanteissa:

9.1.1 merkittävät sääntelypäivitykset (esim. muutokset DORA-asetukseen tai NIS2-direktiiviin)

9.1.2 muutokset haavoittuvuuksien priorisointiviitekehyksissä (esim. CVSS-päivitykset)

9.1.3 merkittävät muutokset IT-ympäristössä (esim. pilvimigraatio tai EDR-ratkaisun uudistus)

9.1.4 merkittävät tietomurrot tai ulkoiset tiedotteet, jotka edellyttävät politiikan vahvistamista

9.2 Katselmoinnin suorittaa tietoturvajohtaja (CISO) yhteistyössä tietoturvavalvonnan, riskienhallinnan ja infrastruktuurijohdon kanssa.

9.3 Politiikan päivitykset on:

9.3.1 dokumentoitava ISMS:n asiakirjahallintarekisteriin

9.3.2 katselmoitava ja hyväksyttävä ylimmän johdon toimesta

9.3.3 viestittävä kaikille asianomaisille sidosryhmille, mukaan lukien kolmannet osapuolet, jotka käsittelevät tietoja

9.4 Historialliset versiot on säilytettävä turvallisesti auditointi- ja osoitusvelvollisuustarkoituksia varten.

10. Liittyvät politiikat ja yhteydet

10.1 P1 - Tietoturvapolitiikka. Määrittää yleisen sitoumuksen järjestelmien ja tietojen suojaamiseen, mukaan lukien haavoittuvuuksien ennakoiva hallinta ja ohjelmistojen eheyden varmistaminen.

10.2 P5 - Muutoksenhallintapolitiikka. Ohjaa kaikkia korjauspäivitysten käyttöönottoja ja konfiguraatiomuutoksia edellyttäen dokumentointia, testausta, hyväksyntää ja palautusmenettelyjä, jotka täydentävät haavoittuvuuksien korjausprosesseja.

10.3 P6 - Riskienhallintapolitiikka. Tukee korjaamatta jääneiden haavoittuvuuksien luokittelua ja käsittelyä rakenteisten riskinarviointien, vaikutusanalyysin ja jäännösriskin hyväksyntämenettelyjen avulla.

10.4 P12 - Omaisuuden hallintapolitiikka. Varmistaa, että järjestelmät inventoidaan ja luokitellaan oikein, mikä mahdollistaa yhdenmukaisen haavoittuvuusskannauksen, omistajuuden määrittämisen ja korjauspäivitysten kattavuuden koko elinkaaren ajan.

10.5 P22 - Lokitus- ja valvontapolitiikka. Määrittää vaatimukset tapahtumien havaitsemiselle ja auditointijäljen muodostamiselle. Tämä politiikka tukee näkyvyyttä paikkaustoimintaan, luvattomiin muutoksiin ja tunnettuihin haavoittuvuuksiin kohdistuviin hyväksikäyttöyrityksiin.

10.6 P30 - Tietoturvapoikkeamien hallintapolitiikka. Määrittää eskalointiprotokollat ja rajaamisstrategiat hyväksikäytettyjä haavoittuvuuksia, tietomurtotutkintoja ja tämän politiikan kontrollien mukaisia korjaavia toimenpiteitä varten.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001: Lauseke 8.1 - toiminnan suunnittelu ja ohjaus: edellyttää teknisten haavoittuvuuksien järjestelmällistä käsittelyä tietoturvakontrollien jatkuvan vaikuttavuuden varmistamiseksi.

11.2 ISO/IEC 27002:2022 - Kontrollit 8.8, 8.9, 5: antaa toteutusohjeet paikkaamiseen, haavoittuvuusskannaukseen, ohjelmistojen eheyteen sekä integrointiin turvallisen konfiguroinnin ja omaisuusluetteloiden kanssa.

11.3 NIST SP 800-53 Rev.5: RA-5 - haavoittuvuuksien seuranta ja skannaus: edellyttää tiheää skannausta ja korjaamisen seurantaa. SI-2 - puutteiden korjaaminen: edellyttää puutteiden viipymätöntä arviointia ja lieventämistä saatavilla olevilla korjauspäivityksillä tai muilla toimenpiteillä. CM-2 / CM-6 - konfiguraationhallinnan perustasot ja kontrollit: muodostaa perustan turvallisille järjestelmäkonfiguraatioille, jotka on sidottu korjauspäivitysten toimeenpanoon.

11.4 EU:n GDPR (2016/679): Artikla 32 - käsittelyn turvallisuus: edellyttää asianmukaisten teknisten toimenpiteiden toteuttamista, kuten viipymätöntä paikkaamista ja haavoittuvuuksien käsittelyä, luottamuksellisuuden ja järjestelmien häiriönsietokyvyn varmistamiseksi. Johdanto-osan kappale 49: kannustaa organisaatioita ottamaan käyttöön ennaltaehkäiseviä hallintakeinoja tunnettuja uhkia vastaan turvallisuuden ja jatkuvuuden tukemiseksi.

11.5 EU:n NIS2-direktiivi (2022/2555): Artikla 21(2)(d): velvoittaa keskeiset ja tärkeät toimijat havaitsemaan, käsittelemään ja lieventämään järjestelmien haavoittuvuuksia sekä ylläpitämään korkeaa kyberhygienian tasoa.

11.6 EU:n DORA-asetus (2022/2554): Artikla 8 - ICT-riskien hallinta: edellyttää finanssijärjestelmissä käytettävien tieto- ja viestintäteknologioiden haavoittuvuuksien tunnistamista ja oikea-aikaista korjaamista. Artikla 10(2)(f): korostaa jatkuvia uhkalähtöisiä haavoittuvuusarviointeja ja paikkaamista osana toiminnallista häiriönsietokykyä.

11.7 COBIT 2019: DSS05.02 - tietoturvahaavoittuvuuksien hallinta: ohjaa organisaatioita skannaamaan, seuraamaan ja lieventämään tunnettuja teknisiä heikkouksia. DSS01.03 - infrastruktuurin seuranta: varmistaa, että järjestelmiä seurataan hyväksikäytön tai heikkouksien merkkien havaitsemiseksi. MEA03 - vaatimustenmukaisuuden seuranta, arviointi ja tarkastelu: edellyttää kontrollien vaikuttavuuden säännöllistä auditointia, mukaan lukien korjauspäivitysten tila ja poikkeusten käsittely.