					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P13					Asiakirjan nimi: **Tiedon luokittelu- ja merkintäpolitiikka**							
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 Tässä politiikassa määritellään muodollinen viitekehys organisaation tietovarojen luokittelulle ja merkitsemiselle niiden arkaluonteisuuden, riskialtistuksen ja sääntelyvaatimusten perusteella.

1.2 Politiikalla varmistetaan, että kaikki tiedot, riippumatta siitä, säilytetäänkö, siirretäänkö vai käsitelläänkö niitä, luokitellaan ja merkitään selkeästi siten, että niiden edellyttämä suojaustaso ja käsittelyvaatimukset käyvät ilmi.

1.3 Politiikka edellyttää rakenteista luokittelua, joka on yhdenmukainen organisaation riskienhallintakäytäntöjen kanssa ja tukee luottamuksellisuutta, eheyttä ja saatavuutta kaikissa digitaalisissa ja fyysisissä tietomuodoissa.

1.4 Tämä kontrolli on olennainen roolipohjaisen pääsynhallinnan, auditointivalmiuden, asianmukaisen tiedonjaon sekä salausta, varmuuskopiointia ja valvontaa koskevien teknisten suojatoimien tehokkaan käyttöönoton mahdollistamiseksi.

2. Soveltamisala

2.1 Tätä politiikkaa sovelletaan seuraaviin:

2.1.1 Kaikkiin organisaation tietovaroihin, mukaan lukien asiakirjat, tietokannat, tallenteet ja viestintä

2.1.2 Kaikkiin tietomuotoihin, mukaan lukien digitaaliset, painetut, kirjalliset ja suulliset tiedot

2.1.3 Kaikkiin ympäristöihin: omissa tiloissa, etäkäytössä, mobiiliympäristöissä ja pilviympäristöissä

2.1.4 Kaikkiin työntekijöihin, sopimuskumppaneihin, palveluntarjoajiin ja kolmannen osapuolen henkilötietojen käsittelijöihin, jotka luovat, käsittelevät tai säilyttävät organisaation tietoja

2.2 Soveltamisala kattaa sisäisesti tuotetun sisällön, ulkoisista lähteistä saadut tiedot, tietosuojalainsäädännön velvoitteiden alaiset henkilötiedot (esim. EU:n GDPR) sekä asiakkaille, kumppaneille ja viranomaisille luovutettavat tiedot.

2.3 Politiikka koskee kaikkia tietojen säilyttämiseen tai siirtämiseen käytettäviä järjestelmiä, mukaan lukien yrityssovellukset, tiedostopalvelimet, sähköpostijärjestelmät, pilvialustat ja varmuuskopiointivarastot.

3. Tavoitteet

3.1 Määrittää standardoitu, koko organisaation kattava luokittelumalli, joka perustuu tietojen altistumisen tai vaarantumisen vaikutuksiin.

3.2 Varmistaa, että kaikki tiedot merkitään näkyvästi ja pysyvästi siten, että merkintä vastaa luokittelutasoa ja käsittelyvaatimuksia.

3.3 Toteuttaa luokitteluun perustuvat tietojen käsittely- ja pääsynhallintakontrollit, mukaan lukien salaus, lokitus, siirron suojaaminen ja säilytysaikojen hallinta.

3.4 Tukea kansainvälisten standardien (ISO/IEC 27001, 27002), oikeudellisten viitekehysten (EU:n GDPR, EU:n NIS2-direktiivi, EU:n DORA-asetus) sekä sisäisten riskienhallintapolitiikkojen noudattamista.

3.5 Varmistaa, että kaikki käyttäjät ymmärtävät vastuunsa tietojen suojaamisessa, merkintöjen soveltamisessa ja luokiteltujen tietojen asianmukaisessa käsittelyssä.

3.6 Ylläpitää jäljitettävyyttä luokitustilan, siihen liittyvien kontrollien ja organisaation omaisuusrekisterin välillä auditointi- ja vaatimustenmukaisuustarkoituksia varten.

4. Roolit ja vastuut

4.1 Tietoturvajohtaja (CISO)

4.1.1 Vastaa tiedon luokittelu- ja merkintäpolitiikasta ja varmistaa sen yhdenmukaisuuden sääntelyyn, sopimuksiin ja toimintaan liittyvien vaatimusten kanssa.

4.1.2 Hyväksyy luokittelutasot, merkintästandardit ja politiikan muutokset.

4.1.3 Valvoo politiikan noudattamista auditointien, mittareiden ja poikkeamien katselmointien avulla.

4.1.4 Koordinoi poikkitoiminnallista hallinnointia oikeudellisten ja vaatimustenmukaisuustoimintojen, tietosuojan ja riskienhallinnan kanssa.

4.2 Tiedon omistaja

4.2.1 Vastaa hallinnassaan olevien tietovarojen luokittelusta organisaation luokittelumallin mukaisesti.

4.2.2 Soveltaa luokittelumerkintöjä tiedon luomisen, päivittämisen tai vastaanoton yhteydessä.

4.2.3 Katselmoi omaisuuserien luokituksen säännöllisesti erityisesti silloin, kun arkaluonteisuus, sääntelyn soveltamisala tai liiketoiminta-arvo muuttuu.

4.2.4 Varmistaa, että arkaluonteisia tietoja käsitellään ja merkitään asianmukaisesti koko niiden elinkaaren ajan.

[... 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 sen varmistamiseksi, että se on yhdenmukainen seuraavien kanssa:

9.1.1 Kehittyvät sääntelyvaatimukset (esim. EU:n GDPR, EU:n NIS2-direktiivi, EU:n DORA-asetus)

9.1.2 ISO/IEC 27001:n tai 27002:n luokittelua koskevan ohjeistuksen päivitykset

9.1.3 Organisaatiomuutokset, jotka vaikuttavat tietojen arkaluonteisuuteen tai omistajuuteen

9.1.4 Teknologiset muutokset, mukaan lukien uudet asiakirja- tai tiedonhallinta-alustat

9.2 Tietoturvajohtaja (CISO) käynnistää katselmoinnin yhteistyössä tietoturvakomitean, oikeudellisen neuvonnan ja vaikutuksen alaisten liiketoimintayksiköiden kanssa.

9.3 Katselmointien on sisällettävä seuraavat:

9.3.1 Luokittelun valvonnan tehokkuus ja käyttäjien politiikan noudattaminen

9.3.2 Virheelliseen luokitteluun liittyvien poikkeamien ja poikkeusten analyysi

9.3.3 Käyttäjäpalaute merkintätyökaluista tai ohjemateriaaleista

9.3.4 Vertailu toimialan luokittelustandardeihin

9.4 Politiikan päivitysten on oltava versiohallittuja, dokumentoituja ISMS-tietovarastossa ja viestittyjä kaikille asiaankuuluville henkilöille siten, että uudet vastuut tai työkalumuutokset korostetaan.

9.5 Uudet työntekijät on perehdytettävä politiikan voimassa olevaan versioon perehdytyksen aikana. Kaikkien työntekijöiden on suoritettava kertauskoulutus merkittävien politiikkamuutosten jälkeen.

10. Liittyvät politiikat ja yhteydet

10.1 Tätä politiikkaa tukevat suoraan seuraavissa liittyvissä politiikoissa kuvatut kontrollit, ja tämä politiikka toimeenpanee niitä:

10.1.1 P4 - Pääsynhallintapolitiikka: Tietoihin pääsyä hallitaan luokittelutasojen perusteella; mitä arkaluonteisempi tieto, sitä tiukemmat pääsynhallinta- ja valtuutusmekanismit vaaditaan.

10.1.2 P11 - Käyttäjätilien ja etuoikeuksien hallintapolitiikka: Vahvistaa oikeuksien myöntämisen vähimmän oikeuden periaatteen mukaisesti, mitä luokittelutasot ohjaavat.

10.1.3 P12 - Omaisuudenhallintapolitiikka: Varmistaa, että jokaisen omaisuusrekisterissä olevan omaisuuserän yhteydessä on sen luokitus ja merkintä, mikä tukee jäljitettävyyttä ja vastuun osoitettavuutta.

10.1.4 P14 - Tietojen säilytys- ja hävittämispolitiikka: Hävittämis- ja säilytyssäännöt määräytyvät tiedon luokittelutason ja sääntelyn mukaisten säilytysvaatimusten perusteella.

10.1.5 P18 - Kryptografisten kontrollien politiikka: Soveltaa asianmukaisia salausstandardeja tietovaran luokituksen perusteella.

10.1.6 P22 - Lokitus- ja valvontapolitiikka: Mahdollistaa luokiteltujen tietojen käytön ja liikkumisen seurannan varmistaen todennettavuuden sekä virheellisten merkintöjen tai väärinkäytön havaitsemisen.

10.2 Kukin yhteys varmistaa tiedon yhdenmukaisen suojaamisen koko sen elinkaaren ajan tiedon luomisesta ja luokittelusta turvalliseen käsittelyyn, säilytykseen, siirtoon ja lopulliseen tuhoamiseen saakka.

11. Viitestandardit ja viitekehykset

11.1 Tämä politiikka on yhdenmukainen kansainvälisesti tunnustettujen standardien ja sääntelyviitekehysten kanssa, jotka koskevat arkaluonteisten tietojen luokittelua ja merkitsemistä.

11.2 ISO/IEC 27001

11.2.1 Kohta 4.2 - Asianomaisten osapuolten tarpeiden ja odotusten ymmärtäminen. Luokitteluvaatimukset perustuvat usein asianomaisten osapuolten asettamiin oikeudellisiin, sääntelyyn liittyviin tai sopimuksellisiin velvoitteisiin (esim. EU:n GDPR, asiakkaiden salassapitosopimukset (NDA)), jotka on otettava huomioon tässä politiikassa.

11.2.2 Kohta 6.1.3 - Tietoturvariskien käsittely. Luokittelu vaikuttaa suoraan riskienkäsittelyssä käytettävien kontrollien valintaan, mukaan lukien pääsynhallinta, salaus ja säilytys tiedon arkaluonteisuuden perusteella.

11.2.3 Kohta 7.2 - Pätevyys. Politiikka edellyttää, että luokittelusta ja merkitsemisestä vastaavat henkilöt koulutetaan, mikä kuuluu pätevyysvaatimusten piiriin.

11.2.4 Kohta 7.3 - Tietoisuus. Politiikka edellyttää, että kaikki käyttäjät tuntevat luokittelutasot ja vastuunsa tietojen käsittelyssä, mikä vastaa tietoisuusvaatimuksia.

11.2.5 Kohta 7.5 - Dokumentoitu tieto. Luokittelupolitiikka itsessään on hallittu asiakirja, ja menettelyt, koulutustiedot sekä luokittelumerkinnät kuuluvat dokumentoidun tiedon piiriin.

11.2.6 Kohta 8.1 - Toiminnan suunnittelu ja ohjaus. Luokittelu ja merkitseminen ovat operatiivisia prosesseja, jotka on sisällytetty tiedon elinkaaren hallintaan, ja tämä kohta varmistaa, että tällaiset toiminnot suunnitellaan, toteutetaan ja hallitaan.

11.2.7 Kohta 9.1 - Seuranta, mittaaminen, analysointi ja arviointi. Politiikka sisältää määräykset luokittelun noudattamisen, poikkeamatrendien ja merkintämallin tehokkuuden seurannasta.

11.2.8 Kohta 10.1 - Poikkeama ja korjaavat toimenpiteet. Politiikassa määritellään reagointitavat virheelliseen luokitteluun, mukaan lukien korjaavat toimenpiteet kuten uudelleenkoulutus, päivitykset ja poikkeusten käsittely.

11.3 ISO/IEC 27002:2022

11.3.1 Kontrolli 5.12 - Tiedon luokittelu. Tämä kontrolli varmistaa, että tiedot luokitellaan niiden arkaluonteisuuden, arvon ja kriittisyyden perusteella, mikä on tämän politiikan tarkoitus.

11.3.2 Kontrolli 5.13 - Tiedon merkitseminen. Tämä kontrolli edellyttää tiedon asianmukaista merkitsemistä sen luokittelutason mukaisesti, mikä käsitellään tässä politiikassa kattavasti.

11.3.3 Kontrolli 5.10 - Tiedon ja muiden siihen liittyvien omaisuuserien hyväksyttävä käyttö. Politiikka määrittää, miten käyttäjien on käsiteltävä luokiteltuja tietoja, tukee suoraan hyväksyttävää käyttöä ja ehkäisee väärinkäyttöä.

11.3.4 Kontrolli 5.11 - Omaisuuden palautus. Luokittelu auttaa varmistamaan, että arkaluonteiset tiedot tunnistetaan ja palautetaan tai puhdistetaan turvallisesti työntekijän tai toimittajan poistuessa.

11.3.5 Kontrolli 5.9 - Tiedon ja muiden siihen liittyvien omaisuuserien inventointi. Luokittelu kytkeytyy usein omaisuusrekisteriin, jossa on näkyttävä kunkin kohteen luokittelutaso asianmukaisen kontrollien kohdentamisen tukemiseksi.

11.3.6 Kontrolli 5.14 - Tiedonsiirto. Luokittelutasot vaikuttavat sisäisten ja ulkoisten tiedonsiirtojen kontrolleihin (esim. salaus, hyväksyntä, käyttöoikeusrajoitukset).

11.3.7 Kontrolli 8.12 - Tietovuotojen estäminen. Luokittelun ja merkintöjen toteuttaminen tukee luvattoman luovuttamisen ja tietojen menetyksen estämistä.

11.3.8 Kontrolli 8.11 - Tietojen peittäminen. Tietyt luokittelutasot (esim. Luottamuksellinen, Rajoitettu) voivat edellyttää peittämistä, kun tietoja käytetään testi- ja kehitysympäristöissä tai analytiikassa.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-2 - Järjestelmien ja viestinnän suojaamista koskeva politiikka ja menettelyt: tukee luokittelupolitiikkoja osana yleistä tietosuojan kokonaisuutta.

11.4.2 AC-16 - Tietoturva-attribuutit: toteuttaa pääsyn valvonnan luokittelun metatietojen ja käyttäjien käyttöoikeuksien perusteella.

11.4.3 MP-3 / MP-5 - Tietovälineiden merkitseminen ja kuljetuksen suojaus: toteuttaa lepotilassa olevien ja siirrettävien tietojen merkinnän ja suojauksen luokituksen perusteella.

11.5 EU:n GDPR (2016/679)

11.5.1 Artikla 5 - Tietosuojaperiaatteet: edellyttää henkilötietojen turvallista käsittelyä suhteessa niiden arkaluonteisuuteen.

11.5.2 Artikla 32 - Käsittelyn turvallisuus: vahvistaa luokittelun riskiperusteisen tietosuojan ja asianmukaisten teknisten toimenpiteiden mekanismina.

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

11.6.1 Artikla 21(2)(a): edellyttää tietoturvariskien hallintaa koskevia politiikkoja, mukaan lukien omaisuuden ja tietojen luokittelun kontrollit.

11.6.2 Artikla 21(3): kannustaa ottamaan käyttöön asianmukaisia tietojen käsittelyä varmistavia toimenpiteitä, joita tuetaan luokitteluun perustuvalla merkitsemisellä.

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

11.7.1 Artikla 5 - Hallinnointi ja valvonta: edellyttää hallinnointiviitekehystä, jossa tieto-omaisuus luokitellaan ICT-riskien hallintaa varten.

11.7.2 Artikla 9 - ICT-riskien hallinta: asettaa kriittisiä ICT-omaisuuseriä koskevia teknisiä ja organisatorisia toimenpiteitä, mukaan lukien luokittelu ja merkitseminen.

11.8 COBIT 2019

11.8.1 DSS05.02 - Tietoturvapalveluiden hallinta: edellyttää tiedon luokittelua yrityksen tietojen suojaamisen varmistamiseksi.

11.8.2 MEA03 - Vaatimustenmukaisuuden seuranta, arviointi ja arvioiminen: tukee luokittelukäytäntöjen säännöllistä auditointia ja katselmointia politiikan noudattamisen ja kypsyystason varmistamiseksi.