					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P13S					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**

Yhdenmukaisuus standardien ja sääntelyvaatimusten kanssa

Standardi/sääntely	Lauseke/artikla	Kommentti
ISO/IEC 27001:2022	Kohdat 5.3, 8	
ISO/IEC 27002:2022	Kontrollit 5.12, 5.13	
NIST SP 800-53 Rev.5	AC-16, MP-3, MP-5	
EU:n NIS2-direktiivi	Artikla 21(2)(a)	
EU:n DORA-asetus	Artikla 5(8)	
COBIT 2019	BAI03.05, DSS05	
EU:n GDPR	Artiklat 5, 32	

1. Tarkoitus

1.1 Tämä politiikka määrittää, miten kaikki organisaation käsittelemä tieto on luokiteltava ja merkittävä siten, että sen luottamuksellisuus, eheys ja saatavuus säilyvät koko elinkaaren ajan.

1.2 Politiikan tarkoituksena on varmistaa yhdenmukaiset tiedonkäsittelykäytännöt määrittämällä tiedolle asianmukaiset suojaustasot sen arkaluonteisuuden, liiketoimintavaikutuksen tai oikeudellisten velvoitteiden perusteella.

1.3 Luokittelu ja merkintä auttavat vähentämään tahattoman paljastumisen, luvattoman pääsyn ja arkaluonteisten tietojen virheellisen käsittelyn riskiä erityisesti pk-yrityksissä, joissa voidaan tukeutua yksinkertaisempiin järjestelmiin ja vähemmän formalisoituihin kontrollitoimiin.

1.4 Tämä politiikka on keskeinen ISO/IEC 27001 -sertifioinnin ja sääntelyvaatimusten noudattamisen kannalta erityisesti tietosuojalainsäädännön, kuten GDPR:n, sekä kyberturvallisuuden viitekehysten, kuten NIS2:n ja DORA:n, osalta.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkea organisaation tietoa sen muodosta tai sijainnista riippumatta, mukaan lukien:

2.1.1 sähköiset asiakirjat, laskentataulukot, sähköpostit, lomakkeet, kuvat ja skannatut tiedostot

2.1.2 fyysiset asiakirjat, kuten tulosteet, raportit, laskut ja muistiinpanot

2.1.3 pilvipalveluihin, paikallisille palvelimille, siirrettäville tallennusvälineille tai liiketoiminnassa käytettäville henkilökohtaisille laitteille tallennettu tai niissä käsiteltävä tieto

2.1.4 liiketoiminnan aikana syntyvä väliaikainen tai ohimenevä tieto (esim. lokit, välimuistitiedostot, sähköpostit)

2.2 Kaikkien työntekijöiden, sopimuskumppanien, määräaikaisten työntekijöiden ja ulkoisten palveluntarjoajien, joilla on pääsy organisaation tietoihin, on noudatettava tätä politiikkaa.

2.3 Tätä politiikkaa sovelletaan koko tiedon elinkaaren ajan luonnista ja tallennuksesta käytön ja siirron kautta arkistointiin tai poistamiseen.

3. Tavoitteet

3.1 Määrittää yksinkertainen ja toimeenpantava luokittelumalli, joka on helppo ymmärtää ja ottaa käyttöön koko organisaatiossa.

3.2 Edellyttää, että jokainen tietoaineisto ja tietovaranto luokitellaan sen arkaluonteisuuden perusteella ja merkitään vastaavasti asianmukaisen käsittelyn, säilytyksen ja pääsyn ohjaamiseksi.

3.3 Varmistaa, että tietojen merkintäkäytännöt integroidaan liiketoiminnan työnkulkuihin, kuten perehdytykseen, projektien käynnistämiseen ja järjestelmien käyttöönottoon.

3.4 Vähentää tietomurtojen riskiä soveltamalla luokitustason mukaisia käsittelyyn liittyviä kontrollitoimia (esim. salaus, pääsyn rajoittaminen).

3.5 Varmistaa tietosuojaa ja tietoturvaa koskevien lakien noudattaminen osoittamalla, että arkaluonteinen tieto (esim. henkilötiedot, taloustiedot tai immateriaalioikeuksiin liittyvät tiedot) merkitään asianmukaisesti ja hallitaan oikein.

3.6 Määrittää vastuut luokittelupäätöksistä ja varmistaa säännölliset katselmoinnit ja päivitykset muuttuvien liiketoiminta- ja oikeudellisten tarpeiden perusteella.

4. Roolit ja vastuut

4.1 Toimitusjohtaja

4.1.1 Omistaa tämän politiikan ja hyväksyy luokittelumallin.

4.1.2 Huolehtii valvonnasta varmistaakseen, että luokitteluun liittyvät vastuut on delegoitu ja että niitä noudatetaan.

4.1.3 Katselmoi ja hyväksyy kaikki luokittelu- tai merkintävaatimuksia koskevat poikkeukset.

4.1.4 Varmistaa, että tietojen käsittelykäytännöt täyttävät GDPR:n ja DORA:n kaltaisten säädösten vaatimukset.

4.2 Tiedon omistaja / tietovastaava

4.2.1 Määrittää alkuperäisen luokituksen jokaiselle uudelle tietoaineistolle tai tietovarannolle sen luomisen tai hankinnan yhteydessä.

4.2.2 Varmistaa, että näkyvät merkinnät (esim. tiedoston ylä- ja alatunnisteet, vesileimat, kansioiden nimet) otetaan käyttöön soveltuvin osin.

4.2.3 Katselmoi luokitukset säännöllisesti varmistaakseen niiden ajantasaisuuden, oikeellisuuden ja tarvittavat muutokset (esim. luokituksen alentamisen tai tiedon julkaisun jälkeen).

4.2.4 Tekee yhteistyötä IT-vastaavan kanssa luokitukseen perustuvien teknisten suojaustoimenpiteiden toteuttamiseksi (esim. käyttöoikeudet, salaus).

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Toimitusjohtajan ja tietovastaavan on katselmoitava tämä politiikka vuosittain sen varmistamiseksi, että se vastaa seuraavia:

9.1.1 muutokset liiketoiminnassa tai tietotyypeissä

9.1.2 uudet sääntelyvaatimukset (esim. tietosuojaan tai taloudelliseen valvontaan liittyvät vaatimukset)

9.1.3 teknologiamuutokset, jotka vaikuttavat merkintä- tai luokittelukyvykkyyksiin

9.2 Katselmoinnin on sisällettävä päivitykset luokitteluluokkiin, merkintätyökaluihin tai -käytäntöihin sekä tietoisuus- ja koulutussisältöön.

9.3 Politiikan muutokset on hyväksytettävä toimitusjohtajalla ja viestittävä kaikille työntekijöille. Versiomuutoksista on säilytettävä kirjaus auditointitarkoituksia varten.

10. Liittyvät politiikat ja yhteydet

10.1 P2S – Hallintoroolien ja vastuiden politiikka: määrittää vastuut politiikan omistajuudelle ja soveltamiselle.

10.2 P4S – Pääsynhallintapolitiikka: yhdenmukaistaa järjestelmien käyttöoikeudet tiedon luokittelutasojen kanssa.

10.3 P12S – Omaisuudenhallintapolitiikka: seuraa fyysisiä ja digitaalisia omaisuuseriä, joihin luokiteltua tietoa tallennetaan.

10.4 P17S – Tietosuoja- ja yksityisyydensuojapolitiikka: ohjaa henkilötietojen suojaamista, joista suuri osa on luokiteltu luottamukselliseksi.

10.5 P30S – Tietoturvapoikkeamien hallintapolitiikka: määrittää eskalointipolut ja reagointimenettelyt luokittelurikkomusten tai tiedon altistumisen tapauksissa.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Kohta 5.3: edellyttää selkeästi määriteltyjä vastuita tietojen käsittelylle ja suojaamiselle.

11.1.2 Kohta 8.1: edellyttää toiminnan suunnittelua ja kontrollitoimia, mukaan lukien tiedon luokitteluun liittyvät kontrollit.

11.2 ISO/IEC 27002

11.2.1 Kontrolli 5.12: antaa ohjeistusta tiedon luokittelusta riskien ja sääntelyvaatimusten perusteella.

11.2.2 Kontrolli 5.13: kuvaa käytännön merkintämekanismeja ja niihin liittyviä käsittelysääntöjä.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-16: edellyttää tiedon merkitsemistä sen varmistamiseksi, että suojaustoimenpiteet vastaavat luokitusta.

11.3.2 MP-3 / MP-5: antavat ohjeistusta tallennusvälineiden ja tulosteiden merkitsemisestä ja hallinnasta.

11.4 EU:n GDPR

11.4.1 Artiklat 5 ja 32: edellyttävät tietojen minimointia sekä eheyden ja luottamuksellisuuden varmistamista asianmukaisella luokittelulla ja tietojen käsittelyyn liittyvillä suojaustoimilla.

11.5 EU:n NIS2-direktiivi

11.5.1 Artikla 21(2)(a): velvoittaa toteuttamaan riskiperusteisia teknisiä ja organisatorisia kontrollitoimia tietojen suojaamiseksi.

11.6 EU:n DORA-asetus

11.6.1 Artikla 5(8): edellyttää, että organisaatiot luokittelevat tietovaransa osana ICT-riskien hallintaa.

11.7 COBIT 2019

11.7.1 BAI03.05: edellyttää tiedon luokittelua ja riskiin suhteutettua suojausta.

11.7.2 DSS05.02: käsittelee luokitukseen perustuvien kontrollien soveltamista ja seurantaa.