					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P36S					Asiakirjan nimi: **Sosiaalisen median ja ulkoisen viestinnän 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/säädös	Kohta/artikla	Kommentti
ISO/IEC 27001:2022	Kohta 8	Määritellyt prosessit ja roolipohjainen hallinnointi julkisen viestinnän hallintaan siten, että varmistetaan oikeellisuus, hyväksyntätyönkulut ja poikkeamien eskalointi.
ISO/IEC 27002:2022	Kontrollit 5.10, 5.11, 5.35, 5.36	Ohjaa käyttöä, hyväksyttävää käyttöä sekä ulkoisia yhteydenottoja, viranomaisviestintää ja vaatimustenmukaisuuden raportointia.
NIST SP 800-53 Rev.5	AC-8, AU-12, PL-4	Säännöt järjestelmien ja viestinnän käytölle, käyttäjäilmoituksille sekä auditointitallenteiden säilyttämiselle.
EU:n GDPR	Artiklat 5, 25, 32, 33	Henkilötietojen käsittelyn periaatteet, sisäänrakennettu ja oletusarvoinen tietosuoja, käsittelyn turvallisuus sekä tietoturvaloukkauksia koskevat ilmoitusvelvoitteet.
EU:n NIS2-direktiivi	Artikla 21	Kyberturvallisuusriskien hallintatoimenpiteet sekä poikkeamia ja riskeihin liittyvää julkista viestintää koskevat velvoitteet.
EU:n DORA-asetus	Artiklat 9, 16	ICT-riskien hallinta ja kriittisiä palveluntarjoajia koskeva viestintästrategia.
COBIT 2019	APO09, DSS05	Palvelusopimusten ja viestinnän hallinnointi sekä turvalliset viestintäkäytännöt ja poikkeamien hallinta.

1. Tarkoitus

1.1 Tämä politiikka määrittää pakolliset säännöt ja vastuut, jotka koskevat sosiaalisen median käyttöä ja kaikkea organisaation henkilöstön harjoittamaa ulkoista viestintää.

1.2 Politiikka varmistaa, että julkinen viestintä — suunniteltu tai spontaani — on oikeellista, asianmukaista, turvallista, lainmukaista ja brändin mukaista.

1.3 Politiikan tavoitteena on minimoida mainevahinkoihin, sääntelyrikkomuksiin, immateriaalioikeuksien vuotamiseen ja luvattomiin paljastuksiin liittyvät riskit julkisissa kanavissa.

1.4 Lisäksi politiikka edistää vastuiden selkeyttä ja jäsenneltyä hallinnointia kaikessa organisaatioon liittyvässä tai siihen vaikuttavassa digitaalisessa viestinnässä.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia työntekijöitä, urakoitsijoita, harjoittelijoita ja kolmansien osapuolten edustajia, jotka:

2.1.1 viestivät organisaation puolesta virallisesti tai epävirallisesti

2.1.2 viittaavat organisaatioon tai antavat ymmärtää olevansa siihen sidoksissa julkisessa yhteydessä

2.1.3 käyttävät henkilökohtaisia tai yrityksen tilejä osallistuessaan organisaatiota koskevaan julkiseen keskusteluun

2.2 Tämän politiikan piiriin kuuluvat viestintäkanavat sisältävät muun muassa seuraavat:

2.2.1 sosiaalisen median alustat (esim. LinkedIn, X/Twitter, Instagram, TikTok, YouTube, Facebook)

2.2.2 blogit, wikit, foorumit ja julkiset keskustelupalstat

2.2.3 sähköposti tai suorat viestit ulkoisille osapuolille (esim. asiakkaille, viranomaisille, medialle)

2.2.4 lehdistöhaastattelut, paneelikeskustelut tai tallennetut mediaesiintymiset

2.2.5 osallistuminen verkkoyhteisöihin, joissa organisaatio mainitaan

2.3 Tämä politiikka koskee sekä reaaliaikaista että ennalta ajastettua sisältöä ja soveltuu kaikkiin laitteisiin ja tileihin (henkilökohtaisiin tai yrityksen), joita käytetään viestinnän julkaisemiseen.

3. Tavoitteet

3.1 Estää luottamuksellisten, arkaluonteisten tai sääntelyn alaisten tietojen tahaton tai tahallinen paljastaminen ulkoisten viestintäkanavien kautta.

3.2 Varmistaa, että viralliset julkiset lausunnot ja sosiaalisen median sisältö ovat oikeellisia, valtuutettuja ja yhdenmukaisia yrityksen brändin, eettisten periaatteiden ja strategisen viestinnän kanssa.

3.3 Estää mainevahingot ja varmistaa viestinnän johdonmukaisuus organisaation sisäisten yksiköiden ja ulkoisten alustojen välillä.

3.4 Noudattaa julkisiin lausuntoihin liittyviä sovellettavia oikeudellisia velvoitteita, mukaan lukien muun muassa EU:n GDPR, EU:n NIS2-direktiivi, EU:n DORA-asetus ja toimialakohtaiset viestintävaatimukset.

3.5 Määrittää selkeät vastuut, sallitut käyttötapaukset ja toimeenpanomenettelyt kaikelle henkilöstölle, joka osallistuu julkisesti näkyvään toimintaan.

4. Roolit ja vastuut

4.1 Markkinointi- tai viestintäjohtaja / viestintävastaava

4.1.1 hyväksyy kaikki viralliset yrityksen viestit ulkoista julkaisua varten

4.1.2 ylläpitää sosiaalisen median sisältökalentereita ja brändin yhdenmukaisuutta koskevia ohjeita

4.1.3 seuraa organisaatioon liittyviä verkkomainintoja ja medianäkyvyyttä

4.2 tietoturvajohtaja (CISO) / tietoturvatiimi

4.2.1 seuraa digitaalisia alustoja tietovuotojen, identiteetin väärinkäytön tai tietojenkalasteluyritysten indikaattoreiden havaitsemiseksi

4.2.2 koordinoi tietoturvapoikkeamien hallintaa reagointitiimien kanssa, jos kyseessä on sosiaalisen median kautta toteutettu hyökkäys tai tietoturvaloukkaus

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

9. Toimeenpano ja vaatimustenmukaisuus

9.1 Tämä politiikka on pakollinen kaikelle sen soveltamisalaan kuuluvalle henkilöstölle ja kolmansille osapuolille. Noudattamatta jättäminen voi johtaa seuraaviin toimenpiteisiin:

9.1.1 kirjallinen varoitus

9.1.2 tilapäinen tai pysyvä käyttöoikeuksien poistaminen alustoihin tai järjestelmiin

9.1.3 kurinpidolliset toimenpiteet, mukaan lukien työsuhteen päättäminen

9.1.4 oikeudelliset toimenpiteet, jos ulkoinen viestintä johtaa mainevahinkoon, henkilötietojen tietoturvaloukkaukseen tai sääntelyvaatimusten noudattamatta jättämiseen

9.2 Kurinpidolliset toimenpiteet

9.2.1 Sisäiset rikkomukset (esim. luottamuksellisten tietojen vuotaminen tai organisaation halventaminen) johtavat henkilöstöhallinnon osallistumiseen, muodolliseen tutkintaan ja dokumentointiin työntekijän tietoihin.

9.2.2 Tarvittaessa laki- ja vaatimustenmukaisuustoiminto ryhtyy siviilioikeudellisiin toimenpiteisiin tai ilmoittaa viranomaisille rikollisesta toiminnasta (esim. identiteetin väärinkäyttö, sisäpiiritiedon vuotaminen).

9.3 Vaatimustenmukaisuuden seuranta

9.3.1 Tietoturva- ja viestintätiimien on suoritettava jatkuvaa seurantaa seuraavista:

9.3.1.1 brändimaininnat keskeisillä alustoilla

9.3.1.2 yrityksen kuvamateriaalin tai tavaramerkkien epävirallinen käyttö

9.3.1.3 tunnetut riskit (esim. tyytymättömät työntekijät, identiteetin väärinkäyttöyritykset)

9.3.2 Seuranta on toteutettava työntekijöiden tietosuojaa koskevien lakien ja säädösten mukaisesti, ja kaikki havaitut tapaukset on varmennettava ihmisen tekemällä arvioinnilla.

9.4 Ilmoittajansuoja ja väärinkäytösten ilmoittaminen

9.4.1 Työntekijää, joka epäilee tämän politiikan rikkomista, kannustetaan ilmoittamaan asiasta tietoturvatiimille, laki- ja vaatimustenmukaisuustoiminnolle tai anonyymisti ilmoituskanavan kautta.

9.4.2 Vastatoimet ilmoituksen tekijää kohtaan ovat ehdottomasti kiellettyjä ja johtavat välittömiin kurinpidollisiin toimenpiteisiin.

10. Katselmointi- ja päivitysvaatimukset

10.1 Tämä politiikka on katselmoitava vuosittain tai aiemmin, jos:

10.1.1 sääntelyvaatimuksissa tapahtuu merkittäviä muutoksia (esim. uutta EU:n digitaalista viestintää koskevaa sääntelyä)

10.1.2 käyttöön otetaan uusia sosiaalisen median alustoja tai viestintäkanavia

10.1.3 tapahtuu merkittävä poikkeama tai toistuvia rikkomuksia, jotka viittaavat prosessipuutteisiin

10.1.4 viestintä-, laki- tai tietoturvatoiminnoissa tapahtuu rakenteellinen muutos tai johtovastuun muutos

10.2 Katselmointi on tehtävä yhdessä seuraavien tahojen toimesta:

10.2.1 markkinoinnin / viestinnän johtaja

10.2.2 CISO tai tietoturvariskien vastuuhenkilö

10.2.3 laki- ja vaatimustenmukaisuusvastaavat

10.3 Päivitykset on dokumentoitava politiikan muutosrekisteriin ja viestittävä sisäisten tietoisuuskanavien kautta. Jos muutokset ovat olennaisia, kaikkien asianomaisten henkilöiden on kuitattava politiikka uudelleen.

11. Liittyvät politiikat ja yhteydet

11.1 Tätä politiikkaa tukevat ja siihen liittyvät seuraavat organisaation tietoturvallisuuden hallintajärjestelmän (ISMS) osat:

11.1.1 P1 – Tietoturvapolitiikka: Määrittää tiedon suojaamisen yleiset periaatteet, joihin kuuluu sen varmistaminen, ettei viestintä johda luvattomaan paljastamiseen.

11.1.2 P3 – Hyväksyttävän käytön politiikka: Määrittää digitaalisia alustoja ja teknologioita koskevan hyväksyttävän toiminnan, joka ohjaa suoraan sosiaalisten kanavien henkilökohtaista ja ammatillista käyttöä.

11.1.3 P6 – Riskienhallintapolitiikka: Tarjoaa riskienhallinnan viitekehyksen julkiseen viestintään ja mainealtistukseen liittyvien uhkien arviointiin.

11.1.4 P8 – Tietoturvatietoisuus- ja koulutuspolitiikka: Määrittää tietoisuusohjelmat, joilla henkilöstöä koulutetaan turvallisiin viestintäkäytäntöihin ja sosiaalisen manipuloinnin uhkiin.

11.1.5 P13 – Tiedon luokittelu- ja merkintäpolitiikka: Ohjaa henkilöstöä siinä, mitä pidetään rajoitettuna tai luottamuksellisena tietona, jota ei saa paljastaa ulkoisesti.

11.1.6 P30 – Tietoturvapoikkeamien hallintapolitiikka: Määrittää, miten julkiseen viestintään liittyviä poikkeamia, mukaan lukien tietovuodot, identiteetin väärinkäyttö ja sääntelyrikkomukset, käsitellään.

11.1.7 P33 – Auditointi- ja vaatimustenmukaisuuden seurantapolitiikka: Ohjaa auditointiprosesseja, joilla varmennetaan sosiaalisen median kontrollit, valvontajärjestelmät ja ulkoista viestintää koskevien politiikkojen noudattaminen.

12. Viitestandardit ja viitekehykset

12.1 ISO/IEC 27001:

12.1.1 Kohta 8.1 – Operatiivinen suunnittelu ja ohjaus: Edellyttää määriteltyjä prosesseja ja roolipohjaista hallinnointia julkisen viestinnän hallintaan sekä oikeellisuuden, hyväksyntätyönkulkujen ja tieto- tai maineriskiä koskevien poikkeamien eskaloinnin varmistamista.

12.2 ISO/IEC 27002:2022:

12.2.1 Kontrolli 5.10 – Tiedon käyttö: Ohjaa sisäisen ja ulkoisen viestinnän valtuutettua ja eettistä jakamista.

12.2.2 Kontrolli 5.11 – Tiedon ja omaisuuden hyväksyttävä käyttö: Vahvistaa hyväksyttävät käytännöt sisällön jakamiseen yrityksen omaisuuseriä tai henkilökohtaisia tilejä käyttäen.

12.2.3 Kontrolli 5.35 – Yhteydenpito viranomaisiin: Edellyttää jäsenneltyä ja valtuutettua ulkoista viestintää sääntelyviranomaisille ja julkisille toimijoille.

12.2.4 Kontrolli 5.36 – Politiikkojen ja standardien noudattaminen: Edellyttää sisäisten politiikkojen johdonmukaista soveltamista kaikissa viestintätilanteissa.

12.3 NIST SP 800-53 Rev.5:

12.3.1 PL-4 – Käyttäytymissäännöt: Edellyttää muodollisia sääntöjä järjestelmien ja viestinnän käytölle, mukaan lukien julkistamista koskevat standardit.

12.3.2 AC-8 – Järjestelmän käyttöä koskeva ilmoitus: Tukee pakollisia vastuuvapauslausekkeita ja sisältövaroituksia ulkoisilla alustoilla.

12.3.3 AU-12 – Auditointitallenteiden säilyttäminen: Koskee lokien ja viestintähistorian säilyttämistä poikkeamien katselmointia ja auditointitarkoituksia varten.

12.4 EU:n GDPR (2016/679):

12.4.1 Artikla 5 – Henkilötietojen käsittelyn periaatteet: Kieltää henkilötietojen luvattoman jakamisen julkisen viestinnän kautta.

12.4.2 Artikla 25 – Sisäänrakennettu ja oletusarvoinen tietosuoja: Edellyttää tietosuojan suojatoimia viestintätyökaluissa ja sisällön työnkuluissa.

12.4.3 Artikla 32 – Käsittelyn turvallisuus: Koskee salausta, pääsynhallintaa ja sisällön hyväksyntäprosesseja.

12.4.4 Artikla 33 – Tietoturvaloukkauksista ilmoittaminen: Edellyttää henkilötietojen vuotamisesta ilmoittamista ajallaan, myös silloin kun vuoto tapahtuu julkisten kanavien kautta.

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

12.5.1 Artikla 21 – Kyberturvallisuusriskien hallintatoimenpiteet: Sisältää viestintäprotokollat ja velvoitteet poikkeamatilanteissa sekä riskejä koskevassa julkisessa viestinnässä.

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

12.6.1 Artikla 9 – ICT-riskien hallinta: Soveltuu ulkoisesti laukaistuihin viestintäriskeihin, kuten identiteetin väärinkäyttöön, virheelliseen tietoon ja maineen häirintään.

12.6.2 Artikla 16 – Viestintästrategia: Edellyttää, että kriittiset finanssialan toimijat tai palveluntarjoajat hallitsevat viestintäriskejä ja reagointia kriisitilanteissa.

12.7 COBIT 2019:

12.7.1 APO09 – Hallitut palvelusopimukset ja viestintä: Edellyttää jäsenneltyä hallinnointia sisäisessä ja ulkoisessa viestinnässä.

12.7.2 DSS05 – Tietoturvapalvelujen hallinta: Varmistaa, etteivät viestintätoimet aiheuta lisäriskiä tai heikennä poikkeamien käsittelyprosesseja.