					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/sääntely	Lauseke/artikla	Kommentti
ISO/IEC 27001:2022	Lausekkeet 5.1, 5.2, 6.1, 8	Johtajuus, riskienhallinta ja ulkoisen viestinnän operatiivinen hallinta
ISO/IEC 27002:2022	Kontrollit 5.10, 5.11	hyväksyttävä käyttö ja tietoturvallisuus viestinnässä
NIST SP 800-53 Rev.5	PL-4, AU-7, IR-6, AC-22	käyttäytymissäännöt, auditointi, poikkeamien ilmoittaminen sekä julkisen sisällön ja pääsyn hallinta
EU:n yleinen tietosuoja-asetus (GDPR)	Artiklat 5, 32, 33	tietosuojaperiaatteet, käsittelyn turvallisuus ja julkiseen viestintään vaikuttavien tietoturvaloukkausten ilmoittaminen
EU:n NIS2-direktiivi	Artikla 21(2)(e), 21(2)(f)	tietojärjestelmien käyttöä koskevat politiikat sekä toimitusketjuun ja julkiseen viestintään liittyvien riskien hallinta
EU:n DORA-asetus	Artikla 14(4)	viestintävelvoitteet poikkeamien jälkeen

1. Tarkoitus

1.1. Tässä politiikassa määritetään pakolliset vaatimukset kaikelle julkisissa kanavissa tapahtuvalle viestinnälle, mukaan lukien sosiaalisen median käyttö, median kanssa asiointi ja ulkoinen digitaalinen sisältö, kun viestinnässä viitataan yritykseen, sen henkilöstöön, asiakkaisiin, järjestelmiin tai sisäisiin toimintatapoihin.

1.2. Politiikan tarkoituksena on suojata yrityksen mainetta, varmistaa lakisääteisten ja sääntelyyn perustuvien vaatimusten noudattaminen sekä vähentää tietovuotojen, virheellisen tiedon levittämisen ja tietoturvapoikkeamien riskiä.

1.3. Politiikka mahdollistaa henkilöstön ja kumppaneiden myönteisen ja vastuullisen osallistumisen verkkokeskusteluihin sekä ehkäisee tahattomia tietojen paljastumisia ja virheellisten mielikuvien syntymistä.

1.4. Politiikka tukee pk-yrityksen valmiutta ISO/IEC 27001 -sertifiointiin käsittelemällä julkisesti tai ulkoisille sidosryhmille saataville asetettavan tiedon hallintaa.

2. Soveltamisala

2.1. Tämä politiikka koskee kaikkia organisaatioon sidoksissa olevia henkilöitä, mukaan lukien:

2.1.1. työntekijät ja urakoitsijat

2.1.2. freelancerit, konsultit ja kolmannet osapuolet

2.1.3. harjoittelijat ja osa-aikainen henkilöstö, joka osallistuu asiakastoimituksiin tai jolla on pääsy järjestelmiin

2.2. Politiikka koskee kaikkia ulkoisen viestinnän muotoja, joissa viitataan organisaatioon, mukaan lukien:

2.2.1. sosiaalisen median julkaisut (LinkedIn, Twitter/X, TikTok, Instagram, Facebook jne.)

2.2.2. blogikirjoitukset, verkkokeskustelufoorumit, asiakasarviot ja keskusteluketjut

2.2.3. esiintymiset (esim. konferenssit, webinaarit, podcastit)

2.2.4. sähköpostit ja viestit toimittajille, viranomaisedustajille tai vaikuttajille

2.2.5. työympäristöistä julkisesti jaetut kuvakaappaukset, valokuvat ja videot

2.3. Politiikkaa sovelletaan myös silloin, kun tällainen viestintä tapahtuu:

2.3.1. henkilökohtaisilta laitteilta tai tileiltä

2.3.2. tavanomaisen työajan ulkopuolella

2.3.3. ilman pahantahtoista tarkoitusta; myös tahattomat tai ohimennen esitetyt kommentit kuuluvat soveltamisalaan, jos niissä viitataan yritykseen

3. Tavoitteet

3.1. Maineen suojaaminen: estetään yrityksen maineen vahingoittuminen luvattoman tai epäasianmukaisen julkisen viestinnän seurauksena

3.2. Tietoturva: estetään arkaluonteisten tietojen, sisäisten järjestelmien tai asiakastietojen tahaton paljastuminen sosiaalisessa mediassa tai julkisissa kanavissa

3.3. Lakien ja sääntelyn noudattaminen: varmistetaan, että kaikki yritykseen viittaava julkinen sisältö noudattaa sovellettavia tietosuojaa ja liiketoimintaviestintää koskevia vaatimuksia

3.4. Ammattimainen toiminta: edistetään vastuullista osallistumista verkkokeskusteluihin ja median kanssa asiointiin myös henkilökohtaisilla tileillä

3.5. Valmius poikkeamatilanteisiin: määritetään selkeät ja toteuttamiskelpoiset toimintavaiheet tahattomien paljastumisten tai politiikkarikkomusten varalle

4. Roolit ja vastuut

4.1. toimitusjohtaja

4.1.1. vastaa tämän politiikan omistajuudesta ja hyväksyy sen

4.1.2. katselmoi ja hyväksyy kaikki julkiset kannanotot, median kanssa tehtävät yhteistyöt ja mediahaastattelut

4.1.3. varmistaa, että tämä politiikka viestitään selkeästi kaikille työntekijöille ja kolmansille osapuolille

4.1.4. tutkii tämän politiikan rikkomukset ja reagoi niihin yhteistyössä tietoturvapoikkeamien hallintamenettelyjen kanssa

4.2. nimetty työntekijä tai viestintävastaava (jos nimetty)

4.2.1. tukee toimitusjohtajaa katselmoimalla sisällön ennen ulkoista julkaisemista, kuten blogikirjoitukset ja puheenvuorojen aiheet

4.2.2. ylläpitää lokia hyväksytystä mediatoiminnasta tai korkean riskin sosiaalisen median julkaisuista

4.2.3. seuraa mahdollisuuksien mukaan verkossa esiintyviä tunnettuja yritystä koskevia mainintoja maine- tai tietoturvariskien havaitsemiseksi

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

9. Katselmointi- ja päivitysvaatimukset

9.1. Vuosittainen katselmointi

9.1.1. Toimitusjohtajan on katselmoitava tämä politiikka vähintään kerran vuodessa

9.1.2. Katselmoinnissa on varmistettava yhdenmukaisuus päivitettyjen lakisääteisten velvoitteiden, alan viestintätrendien ja sisäisten liiketoimintamuutosten kanssa

9.2. Heräteperusteiset katselmoinnit

9.2.1. Tämä politiikka on päivitettävä välittömästi seuraavien jälkeen:

9.2.1.1. merkittävä sosiaalisen median poikkeama tai maineeseen liittyvä ongelma

9.2.1.2. muutos viestintää hallinnoivissa kolmannen osapuolen toimittajissa

9.2.1.3. uusi verkkoviestintää, mediaa tai brändiä koskeva lainsäädäntö tai sääntelyvelvoite

9.3. Muutosten dokumentointi

9.3.1. Kaikki päivitykset on kirjattava, mukaan lukien muutospäivä, muutosten yhteenveto ja toimitusjohtajan hyväksyntä

9.3.2. Auditointi- ja sertifiointitarkoituksia varten on ylläpidettävä versiohistoriaa

9.4. Päivitysten jakelu

9.4.1. Kaikille työntekijöille ja urakoitsijoille on tiedotettava politiikan muutoksista

9.4.2. Päivitetyt versiot on jaettava sähköpostitse tai sisäisten portaalien kautta

9.4.3. Julkista viestintää hoitavan toimittajan on hyväksyttävä päivitetyt ehdot ennen työn jatkamista

10. Liittyvät politiikat ja yhteydet

10.1. Tätä politiikkaa sovelletaan yhdessä seuraavien pk-yrityksen politiikkojen kanssa:

10.1.1. P3S – hyväksyttävän käytön politiikka: määrittää hyväksyttävän toiminnan viestintäalustojen käytössä, mukaan lukien sosiaalisen median käyttö työaikana

10.1.2. P8S – tietoturvatietoisuus- ja koulutuspolitiikka: varmistaa, että henkilöstö on koulutettu tunnistamaan verkossa tapahtuvaan liialliseen jakamiseen, tietojenkalasteluun ja maineeseen kohdistuviin uhkiin liittyvät riskit

10.1.3. P17S – tietosuoja- ja yksityisyydensuojapolitiikka: varmistaa, ettei henkilötietoja tai asiakastietoja jaeta ulkoisessa viestinnässä, yhdenmukaisesti EU:n yleisen tietosuoja-asetuksen (GDPR) ja muiden lakisääteisten vaatimusten kanssa

10.1.4. P30S – Tietoturvapoikkeamien hallintapolitiikka: ohjaa toimintaa sosiaalisen median väärinkäytöstä aiheutuvissa tahattomissa julkisissa paljastuksissa, verkkouhissa tai mainehyökkäyksissä

10.1.5. P37S – laki- ja sääntelyvaatimusten noudattamisen politiikka: määrittää organisaation laajemmat lakisääteiset ja sopimusperusteiset velvoitteet julkista sisältöä jaettaessa

10.2. Näitä politiikkoja on sovellettava yhdessä turvallisen, asiallisen ja lainmukaisen ulkoisen näkyvyyden ylläpitämiseksi.

11. Viitestandardit ja viitekehykset

11.1. ISO/IEC 27001

11.1.1. Lauseke 5.1 – johtajuus ja sitoutuminen: edellyttää johdon valvontaa maineeseen ja tietoon liittyvistä riskeistä

11.1.2. Lauseke 6.1 – riskienhallinta: sisältää viestintään liittyvät riskialtistukset

11.1.3. Lauseke 8.1 – operatiivinen hallinta: kattaa säännöt sille, miten tietoa viestitään ulkoisesti

11.2. ISO/IEC 27002

11.2.1. Kontrolli 5.10 – tietojen ja omaisuuden hyväksyttävä käyttö

11.2.2. Kontrolli 5.11 – tietoturvallisuus viestinnässä

11.3. NIST SP 800-53 Rev. 5

11.3.1. PL-4 – käyttäytymissäännöt: ohjaa asianmukaista toimintaa tietoresurssien käytössä

11.3.2. AU-7 – auditointitietojen vähentäminen ja raporttien tuottaminen: tukee julkisten järjestelmien käytön seurantaa

11.3.3. IR-6 – poikkeamien ilmoittaminen: edellyttää reagointia maineeseen ja viestintään liittyviin loukkauksiin

11.3.4. AC-22 – julkisesti saatavilla oleva sisältö: varmistaa ulkoisten julkaisujen ja pääsyn hallinnan

11.4. EU:n yleinen tietosuoja-asetus (2016/679)

11.4.1. Artikla 5 – henkilötietojen käsittelyä koskevat periaatteet (täsmällisyys, eheys, osoitusvelvollisuus)

11.4.2. Artikla 32 – käsittelyn turvallisuus: edellyttää suojatoimia julkisen jakamisen yhteydessä

11.4.3. Artikla 33 – henkilötietojen tietoturvaloukkauksesta ilmoittaminen: soveltuu, jos henkilötietoja paljastuu ulkoisen viestinnän kautta

11.5. EU:n NIS2-direktiivi (2022/2555)

11.5.1. Artikla 21(2)(e) – tietojärjestelmien käyttöä koskevat politiikat, mukaan lukien viestintäalustat

11.5.2. Artikla 21(2)(f) – politiikat kyberturvallisuusriskien käsittelemiseksi toimitusketjussa ja julkisilla alustoilla

11.6. EU:n DORA-asetus (2022/2554)

11.6.1. Artikla 14(4) – viestintävelvoitteet asiakkaille, kolmansille osapuolille ja viranomaisille operatiivisten poikkeamien jälkeen

11.7. COBIT 2019

11.7.1. APO09 – palvelusopimusten hallinta: kattaa toimittajien ja viestintään liittyvien kolmansien osapuolten valvonnan

11.7.2. DSS05 – tietoturvapalvelujen hallinta: sisältää julkisissa kanavissa näkyvien digitaalisten omaisuuserien suojauksen

11.7.3. EDM03 – riskien optimoinnin varmistaminen: korostaa viestintään liittyvien maine- ja vaatimustenmukaisuusriskien hallintaa