					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P36					Documenttitel: **Beleid inzake sociale media en externe communicatie**							
Versie: 1.0		Ingangsdatum: 01.01.2025			Documenteigenaar:							
X	Beleid		Standaard		Procedure		Formulier		Register		Overig	

Revisiegeschiedenis				
Revisienummer	**Revisiedatum**	**Wijzigingen**	**Beoordeeld door**	**Proceseigenaar**

Goedkeuringen			
Naam	**Functie**	**Datum**	**Handtekening**

Juridische kennisgeving (auteursrecht en gebruiksbeperkingen)

(C) 2025 Clarysec LLC. All rights reserved.

Dit document is intellectueel eigendom van Clarysec LLC. Geen enkel deel van dit document mag zonder voorafgaande uitdrukkelijke schriftelijke toestemming worden gekopieerd, hergebruikt, verspreid of gewijzigd voor commerciële of implementatiedoeleinden.
Ongeautoriseerd gebruik is strikt verboden en kan leiden tot juridische stappen.
Neem voor licentiëring contact op via: info@clarysec.com

Afgestemd op normen en regelgeving

Norm/regelgeving	Clausule/artikel	Opmerking
ISO/IEC 27001:2022	Clausule 8	Gedefinieerde processen en rolgebaseerde governance voor het beheren van publieke communicatie, met borging van juistheid, goedkeuringsworkflows en escalatie van incidenten.
ISO/IEC 27002:2022	Beheersmaatregelen 5.10, 5.11, 5.35, 5.36	Regelt gebruik, aanvaardbaar gebruik en externe communicatie met autoriteiten/contactpersonen, evenals nalevingsrapportage.
NIST SP 800-53 Rev.5	AC-8, AU-12, PL-4	Gedragsregels voor systeem- en communicatiegebruik, gebruikersmeldingen en bewaring van auditlogs.
EU AVG	Artikelen 5, 25, 32, 33	Beginselen van gegevensverwerking, gegevensbescherming by design, beveiliging van verwerking en verplichtingen inzake het melden van inbreuken.
EU NIS2	Artikel 21	Maatregelen voor cyberbeveiligingsrisicobeheer, verplichtingen bij incidenten en risicogerelateerde publieke communicatie.
EU DORA	Artikelen 9, 16	ICT-risicobeheer en communicatiestrategie voor kritieke dienstverleners.
COBIT 2019	APO09, DSS05	Governance van dienstverleningsovereenkomsten en communicatie, evenals veilige communicatiepraktijken en incidentbeheer.

1. Doel

1.1 Dit beleid stelt bindende regels en verantwoordelijkheden vast voor het gebruik van sociale media en alle vormen van externe communicatie door personen die aan de organisatie zijn verbonden.

1.2 Dit beleid waarborgt dat publieke communicatie — gepland of spontaan — juist, respectvol, veilig, juridisch compliant en in lijn met de merkidentiteit is.

1.3 Dit beleid beoogt de risico's te beperken die samenhangen met reputatieschade, niet-naleving van wet- en regelgeving, uitlekken van intellectueel eigendom en ongeautoriseerde openbaarmakingen via publiek toegankelijke kanalen.

1.4 Daarnaast bevordert dit beleid verantwoordingsplicht en een gestructureerde governance voor alle vormen van digitale communicatie waarbij de organisatie betrokken is of die gevolgen heeft voor de organisatie.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle werknemers, contractanten, stagiairs en vertegenwoordigers van derde partijen die:

2.1.1 Namens de organisatie communiceren, formeel of informeel

2.1.2 In een publieke context naar de organisatie verwijzen of de indruk wekken aan de organisatie verbonden te zijn

2.1.3 Persoonlijke of zakelijke accounts gebruiken voor publieke discussies waarbij de organisatie betrokken is

2.2 Onder dit beleid vallende communicatiekanalen omvatten onder meer:

2.2.1 Socialemediaplatforms (bijv. LinkedIn, X/Twitter, Instagram, TikTok, YouTube, Facebook)

2.2.2 Blogs, wiki's, forums en openbare discussieplatforms

2.2.3 E-mail of directe berichten aan externe partijen (bijv. klanten, toezichthouders, media)

2.2.4 Persinterviews, sprekerspanels of opgenomen mediaoptredens

2.2.5 Deelname aan onlinegemeenschappen waarin naar de organisatie wordt verwezen

2.3 Dit beleid geldt voor zowel realtime als vooraf geplande content en is van toepassing op alle apparaten en accounts (persoonlijk of zakelijk) die worden gebruikt om de communicatie te verspreiden.

3. Doelstellingen

3.1 Het voorkomen van onbedoelde of opzettelijke openbaarmaking van vertrouwelijke, gevoelige of gereguleerde informatie via externe communicatiekanalen.

3.2 Het waarborgen dat officiële publieke verklaringen en content op sociale media juist en geautoriseerd zijn en aansluiten bij de merkidentiteit, ethische uitgangspunten en strategische communicatie van de organisatie.

3.3 Het voorkomen van reputatieschade en het afdwingen van consistente berichtgeving over interne afdelingen en externe platforms heen.

3.4 Het voldoen aan toepasselijke wettelijke verplichtingen met betrekking tot publieke verklaringen, waaronder, maar niet beperkt tot, de AVG, NIS2, DORA en sectorspecifieke communicatieregels.

3.5 Het vastleggen van duidelijke verantwoordelijkheden, toegestane gebruikssituaties en handhavingsprotocollen voor al het personeel dat betrokken is bij publiek gerichte activiteiten.

4. Rollen en verantwoordelijkheden

4.1 Chief Marketing Officer of communicatieverantwoordelijke / PR-verantwoordelijke

4.1.1 Keurt alle officiële bedrijfscommunicatie voor externe publicatie goed

4.1.2 Beheert publicatieschema's voor sociale media en richtlijnen voor consistente merkuitingen

4.1.3 Monitort onlinevermeldingen en mediablootstelling met betrekking tot de organisatie

4.2 Chief Information Security Officer (CISO) / informatiebeveiligingsteam

4.2.1 Monitort digitale platforms op indicatoren van datablootstelling, identiteitsnabootsing of phishingpogingen

4.2.2 Coördineert met incidentresponsteams bij aanvallen of inbreuken via sociale media

[... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ...]

9. Handhaving en naleving

9.1 Dit beleid is bindend voor al het onder dit beleid vallende personeel en derde partijen. Niet-naleving kan leiden tot:

9.1.1 Formele waarschuwingen

9.1.2 Tijdelijke of permanente intrekking van toegangsrechten tot platforms of systemen

9.1.3 Disciplinaire maatregelen, waaronder beëindiging van het dienstverband of de opdracht

9.1.4 Gerechtelijke procedures indien externe communicatie leidt tot reputatieschade, een datalek of niet-naleving van regelgeving

9.2 Disciplinaire maatregelen

9.2.1 Interne overtredingen (bijv. het lekken van vertrouwelijke gegevens, smaad jegens de organisatie) leiden tot betrokkenheid van HR, een formeel onderzoek en vastlegging in het personeelsdossier.

9.2.2 Waar van toepassing zal Juridische Zaken civielrechtelijke maatregelen nemen of autoriteiten informeren over strafbare feiten (bijv. identiteitsnabootsing, het lekken van koersgevoelige informatie).

9.3 Nalevingsmonitoring

9.3.1 Het informatiebeveiligingsteam en het communicatieteam moeten doorlopende monitoring uitvoeren van:

9.3.1.1 Merkvermeldingen op grote platforms

9.3.1.2 Onofficieel gebruik van bedrijfsbeelden of handelsmerken

9.3.1.3 Bekende risico's (bijv. ontevreden medewerkers, pogingen tot identiteitsnabootsing)

9.3.2 Monitoring moet voldoen aan wet- en regelgeving inzake werknemersprivacy, waarbij alle gemarkeerde gevallen door een menselijke beoordelaar worden geverifieerd.

9.4 Klokkenluidersmechanisme en melding van misbruik

9.4.1 Elke medewerker die een overtreding van dit beleid vermoedt, wordt aangemoedigd dit te melden aan het informatiebeveiligingsteam, Juridische Zaken of anoniem via het klokkenluidersportaal.

9.4.2 Benadeling van klokkenluiders is strikt verboden en leidt tot onmiddellijke disciplinaire maatregelen.

10. Vereisten voor herziening en actualisering

10.1 Dit beleid moet jaarlijks worden herzien, of eerder indien:

10.1.1 Er significante wijzigingen zijn in wettelijke of regelgevende vereisten (bijv. nieuwe EU-wetgeving voor digitale communicatie)

10.1.2 Nieuwe sociale platforms of communicatiekanalen worden ingevoerd

10.1.3 Er sprake is van een significant incident of herhaalde overtredingen die wijzen op hiaten in processen

10.1.4 Er een structurele wijziging is in de aansturing of inrichting van de PR-, juridische of beveiligingsfunctie

10.2 De herziening moet gezamenlijk worden uitgevoerd door:

10.2.1 Het hoofd Marketing / PR

10.2.2 De CISO of verantwoordelijke voor beveiligingsrisico's

10.2.3 Juridische en complianceverantwoordelijken

10.3 Actualisaties moeten worden vastgelegd in het register voor beleidswijzigingen en worden gecommuniceerd via interne bewustwordingskanalen. Bij materiële wijzigingen moet al het betrokken personeel opnieuw bevestigen van het beleid kennis te hebben genomen.

11. Gerelateerde beleidsdocumenten en samenhang

11.1 Dit beleid wordt ondersteund door en hangt samen met de volgende componenten van het managementsysteem voor informatiebeveiliging (ISMS) van de organisatie:

11.1.1 P1 – Informatiebeveiligingsbeleid: stelt overkoepelende beginselen vast voor de bescherming van informatie, waaronder het waarborgen dat communicatie niet leidt tot ongeautoriseerde openbaarmaking.

11.1.2 P3 – Beleid inzake aanvaardbaar gebruik: definieert aanvaardbaar gedrag voor digitale platforms en technologieën en regelt daarmee rechtstreeks persoonlijk en professioneel gebruik van sociale kanalen.

11.1.3 P6 – Beleid inzake risicobeheer: biedt het risicokader voor het beoordelen van dreigingen die verband houden met publieke communicatie en reputatierisico's.

11.1.4 P8 – Informatiebeveiligingsbewustzijns- en opleidingsbeleid: stelt bewustwordingsprogramma's verplicht die medewerkers informeren over veilige communicatiepraktijken en social-engineeringdreigingen.

11.1.5 P13 – Beleid inzake gegevensclassificatie en etikettering: geeft personeel richting over wat als afgeschermde of vertrouwelijke informatie wordt aangemerkt en dus niet extern openbaar mag worden gemaakt.

11.1.6 P30 – Incidentresponsbeleid: definieert hoe incidenten met betrekking tot publieke communicatie moeten worden afgehandeld, waaronder datalekken, identiteitsnabootsing en niet-naleving van regelgeving.

11.1.7 P33 – Beleid inzake audit- en nalevingsmonitoring: regelt de auditprocessen die beheersmaatregelen voor sociale media, monitoringsystemen en naleving van beleidslijnen voor externe communicatie valideren.

12. Referentienormen en -raamwerken

12.1 ISO/IEC 27001:

12.1.1 Clausule 8.1 – Operationele planning en beheersing: vereist gedefinieerde processen en rolgebaseerde governance voor het beheren van publieke communicatie, met borging van juistheid, goedkeuringsworkflows en escalatie van incidenten die verband houden met gegevens- of reputatierisico.

12.2 ISO/IEC 27002:2022:

12.2.1 Beheersmaatregel 5.10 – Gebruik van informatie: regelt de geautoriseerde en ethische verspreiding van interne of externe communicatie.

12.2.2 Beheersmaatregel 5.11 – Aanvaardbaar gebruik van informatie en andere gerelateerde activa: versterkt aanvaardbare praktijken voor het delen van content met gebruik van bedrijfsmiddelen of persoonlijke accounts.

12.2.3 Beheersmaatregel 5.35 – Contact met autoriteiten: vereist gestructureerde en geautoriseerde externe communicatie met toezichthouders en publieke instanties.

12.2.4 Beheersmaatregel 5.36 – Naleving van beleidslijnen, regels en normen voor informatiebeveiliging: borgt consistente toepassing van interne beleidslijnen in alle communicatiescenario's.

12.3 NIST SP 800-53 Rev.5:

12.3.1 PL-4 – Gedragsregels: vereist formele gedragsregels voor systeem- en communicatiegebruik, waaronder normen voor publieke openbaarmaking.

12.3.2 AC-8 – Kennisgeving over systeemgebruik: ondersteunt verplichte disclaimers en contentwaarschuwingen op extern gerichte platforms.

12.3.3 AU-12 – Bewaring van auditregistraties: is van toepassing op het bewaren van logboeken en communicatiehistorie voor incidentbeoordeling en auditdoeleinden.

12.4 EU AVG (2016/679):

12.4.1 Artikel 5 – Beginselen van gegevensverwerking: verbiedt ongeautoriseerd delen van persoonsgegevens via publieke communicatie.

12.4.2 Artikel 25 – Gegevensbescherming by design en by default: vereist privacywaarborgen in communicatietools en contentworkflows.

12.4.3 Artikel 32 – Beveiliging van verwerking: vereist encryptie, toegangscontrole en contentgoedkeuringsprocessen.

12.4.4 Artikel 33 – Melding van inbreuken: verplicht tot tijdige melding van lekken van persoonsgegevens via publieke kanalen.

12.5 EU NIS2-richtlijn (2022/2555):

12.5.1 Artikel 21 – Maatregelen voor cyberbeveiligingsrisicobeheer: omvat communicatieprotocollen en verplichtingen tijdens incidenten en publieke communicatie over risico's.

12.6 EU DORA (2022/2554):

12.6.1 Artikel 9 – ICT-risicobeheer: is van toepassing op extern geactiveerde communicatierisico's zoals identiteitsnabootsing, desinformatie en reputatieverstoring.

12.6.2 Artikel 16 – Communicatiestrategie: vereist dat kritieke financiële instellingen of dienstverleners communicatierisico's en respons in crisissituaties beheersen.

12.7 COBIT 2019:

12.7.1 APO09 – Beheer van dienstverleningsovereenkomsten en communicatie: vereist gestructureerde governance over interne en externe communicatie.

12.7.2 DSS05 – Beheer van beveiligingsdiensten: waarborgt dat communicatieactiviteiten geen extra risico introduceren en processen voor incidentbeheer niet ondermijnen.