					Voer hier de naam van de geregistreerde rechtspersoon in						
Documentnummer: P36S					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**

Afgestemd op normen en regelgeving

Norm/regelgeving	Clausule/artikel	Opmerking
ISO/IEC 27001:2022	Clausules 5.1, 5.2, 6.1, 8	Leiderschap, risico's en operationele beheersing van externe communicatie
ISO/IEC 27002:2022	Beheersmaatregelen 5.10, 5.11	Aanvaardbaar gebruik en informatiebeveiliging in communicatie
NIST SP 800-53 Rev. 5	PL-4, AU-7, IR-6, AC-22	Gedragsregels, auditing, incidentmelding en beheer van publiek toegankelijke content en toegang
AVG	Artikelen 5, 32, 33	Beginselen inzake gegevensbescherming, beveiliging en melding van inbreuken met impact op openbare communicatie
NIS2-richtlijn	Artikel 21(2)(e), 21(2)(f)	Beleidsregels voor systeemgebruik en risicobeheer in de toeleveringsketen/openbare communicatie
DORA	Artikel 14(4)	Communicatieverplichtingen na incidenten

1. Doel

1.1. Dit beleid stelt bindende richtlijnen vast voor alle extern gerichte communicatie, waaronder het gebruik van sociale media, perscontacten en externe digitale content, wanneer daarin wordt verwezen naar de organisatie, haar medewerkers, klanten, systemen of interne werkwijzen.

1.2. Dit beleid ondersteunt de bescherming van de reputatie van de organisatie, borgt juridische en regelgevende naleving en beperkt het risico op informatielekken, misinformatie en beveiligingsincidenten.

1.3. Dit beleid stelt medewerkers en partners in staat op een positieve en verantwoorde wijze deel te nemen aan online discussies, terwijl onbedoelde openbaarmakingen en onjuiste beeldvorming worden voorkomen.

1.4. Dit beleid versterkt de paraatheid van de mkb-organisatie voor ISO/IEC 27001-certificering door beheersing te waarborgen over informatie die beschikbaar wordt gesteld aan het publiek of aan externe stakeholders.

2. Reikwijdte

2.1. Dit beleid is van toepassing op alle aan de organisatie verbonden personen, waaronder:

2.1.1. werknemers en contractanten

2.1.2. freelancers, consultants en externe leveranciers

2.1.3. stagiairs of parttime medewerkers die betrokken zijn bij dienstverlening aan klanten of toegang hebben tot systemen

2.2. Dit beleid is van toepassing op alle vormen van externe communicatie waarin naar de organisatie wordt verwezen, waaronder:

2.2.1. berichten op sociale media (LinkedIn, X, TikTok, Instagram, Facebook enz.)

2.2.2. blogberichten, online fora, klantbeoordelingen en discussiedraden

2.2.3. presentaties en optredens (bijvoorbeeld conferenties, webinars en podcasts)

2.2.4. e-mails of berichten aan journalisten, overheidsvertegenwoordigers of influencers

2.2.5. openbaar gedeelde screenshots, foto's of video's uit werkomgevingen

2.3. Dit beleid is ook van toepassing wanneer dergelijke communicatie plaatsvindt:

2.3.1. via persoonlijke apparaten of accounts

2.3.2. buiten reguliere werktijden

2.3.3. zonder kwaadwillende intentie; ook onbedoelde of terloopse opmerkingen vallen binnen de reikwijdte indien zij naar de organisatie verwijzen

3. Doelstellingen

3.1. Bescherming van de reputatie: voorkomen van imagoschade voor de organisatie door ongeautoriseerde of ongepaste openbare communicatie

3.2. Gegevensbeveiliging: voorkomen van onbedoelde blootstelling van gevoelige informatie, interne systemen of klantgegevens via sociale media of openbare kanalen

3.3. Juridische en regelgevende naleving: waarborgen dat alle openbare content waarin naar de organisatie wordt verwezen voldoet aan toepasselijke wet- en regelgeving op het gebied van gegevensbescherming en zakelijke communicatie

3.4. Professioneel gedrag: bevorderen van verantwoorde deelname aan online discussies en mediaoptredens, ook via persoonlijke accounts

3.5. Incidentparaatheid: voorzien in duidelijke en uitvoerbare stappen voor het geval van onbedoelde openbaarmakingen of beleidsovertredingen

4. Rollen en verantwoordelijkheden

4.1. Algemeen directeur (GM)

4.1.1. is eigenaar van dit beleid en stelt het vast

4.1.2. beoordeelt en autoriseert alle extern gerichte verklaringen, perscontacten en media-interviews

4.1.3. waarborgt dat dit beleid duidelijk wordt gecommuniceerd aan alle werknemers en externe partijen

4.1.4. onderzoekt overtredingen van dit beleid en treedt daartegen op, in afstemming met de procedures voor incidentrespons

4.2. Aangewezen medewerker of communicatieverantwoordelijke (indien aangewezen)

4.2.1. ondersteunt de GM door content voorafgaand aan externe publicatie te beoordelen (bijvoorbeeld blogberichten of onderwerpen voor presentaties)

4.2.2. houdt registraties bij van goedgekeurde media-activiteiten of sociale-mediaberichten met een verhoogd risico

4.2.3. monitort, voor zover de capaciteit dit toelaat, bekende online vermeldingen van de organisatie op reputatie- of beveiligingsrisico's

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

9. Eisen voor herziening en actualisering

9.1. Jaarlijkse herziening

9.1.1. Dit beleid moet ten minste eenmaal per jaar door de algemeen directeur (GM) worden beoordeeld

9.1.2. De beoordeling moet waarborgen dat het beleid in lijn blijft met geactualiseerde juridische verplichtingen, ontwikkelingen in communicatie binnen de sector en interne wijzigingen binnen de organisatie

9.2. Triggergebaseerde beoordelingen

9.2.1. Dit beleid moet onverwijld worden bijgewerkt na:

9.2.1.1. een significant incident op sociale media of een reputatiekwestie

9.2.1.2. een wijziging in externe leveranciers die communicatie beheren

9.2.1.3. nieuwe wetgeving of regelgevende verplichtingen met betrekking tot online communicatie, media of branding

9.3. Documentatie van wijzigingen

9.3.1. Alle updates moeten worden vastgelegd, inclusief datum van herziening, samenvatting van wijzigingen en goedkeuring door de GM

9.3.2. Voor audit- en certificeringsdoeleinden moet een versiehistorie worden bijgehouden

9.4. Verspreiding van updates

9.4.1. Alle medewerkers en contractanten moeten over beleidswijzigingen worden geïnformeerd

9.4.2. Geactualiseerde versies moeten via e-mail of interne portalen worden gedeeld

9.4.3. Iedere leverancier van openbare communicatie moet geactualiseerde voorwaarden erkennen voordat de werkzaamheden worden voortgezet

10. Gerelateerde beleidslijnen en samenhang

10.1. Dit beleid moet in samenhang worden toegepast met de volgende mkb-beleidslijnen:

10.1.1. P3S – Beleid inzake aanvaardbaar gebruik: definieert aanvaardbaar gedrag bij het gebruik van communicatieplatforms, waaronder toegang tot sociale media tijdens werktijd

10.1.2. P8S – Beleid inzake informatiebeveiligingsbewustzijn en opleiding: waarborgt dat medewerkers zijn opgeleid om de risico's van overmatig delen, phishing of online reputatiedreigingen te herkennen

10.1.3. P17S – Beleid inzake gegevensbescherming en privacy: waarborgt dat persoonsgegevens en klantgegevens niet worden gedeeld in externe communicatie, in lijn met de AVG en andere juridische vereisten

10.1.4. P30S – Incidentresponsbeleid: regelt de respons op onbedoelde openbare openbaarmaking, online dreigingen of reputatieaanvallen als gevolg van misbruik van sociale media

10.1.5. P37S – Beleid inzake juridische en regelgevende naleving: stelt de bredere juridische en contractuele verplichtingen van de organisatie vast bij het openbaar delen van content

10.2. Deze beleidslijnen moeten gezamenlijk worden toegepast om een veilige, respectvolle en juridisch conforme externe aanwezigheid te waarborgen.

11. Referentienormen en -kaders

11.1. ISO/IEC 27001

11.1.1. Clausule 5.1 – Leiderschap en betrokkenheid: vereist toezicht door het management op reputatie- en informatierisico's

11.1.2. Clausule 6.1 – Risicobeheer: omvat risicoblootstelling met betrekking tot communicatie

11.1.3. Clausule 8.1 – Operationele beheersing: omvat regels voor de wijze waarop informatie extern wordt gecommuniceerd

11.2. ISO/IEC 27002

11.2.1. Beheersmaatregel 5.10 – Aanvaardbaar gebruik van informatie en activa

11.2.2. Beheersmaatregel 5.11 – Informatiebeveiliging in communicatie

11.3. NIST SP 800-53 Rev. 5

11.3.1. PL-4 – Gedragsregels: regelt passend gedrag bij het gebruik van informatiebronnen

11.3.2. AU-7 – Auditreductie en rapportgeneratie: ondersteunt monitoring van publiek systeemgebruik

11.3.3. IR-6 – Incidentmelding: vereist respons op reputatie- en communicatie-inbreuken

11.3.4. AC-22 – Publiek toegankelijke content: waarborgt beheersing over externe publicaties en toegang

11.4. AVG (EU) 2016/679

11.4.1. Artikel 5 – Beginselen inzake verwerking van persoonsgegevens (juistheid, integriteit, verantwoordingsplicht)

11.4.2. Artikel 32 – Beveiliging van de verwerking: vereist waarborgen rond openbare deling

11.4.3. Artikel 33 – Melding van inbreuken: is van toepassing indien persoonsgegevens via externe communicatie worden blootgesteld

11.5. NIS2-richtlijn (EU) 2022/2555

11.5.1. Artikel 21(2)(e) – Beleidsregels voor het gebruik van informatiesystemen, waaronder communicatieplatforms

11.5.2. Artikel 21(2)(f) – Beleidsregels voor het beheersen van cyberbeveiligingsrisico's in de toeleveringsketen en op openbare platforms

11.6. DORA (EU) 2022/2554

11.6.1. Artikel 14(4) – Communicatieverplichtingen richting klanten, externe partijen en autoriteiten na operationele incidenten

11.7. COBIT 2019

11.7.1. APO09 – Manage Service Agreements: omvat toezicht op leveranciers en communicatiegerelateerde externe partijen

11.7.2. DSS05 – Manage Security Services: omvat bescherming van extern gerichte digitale activa

11.7.3. EDM03 – Ensure Risk Optimization: benadrukt het beheersen van reputatie- en nalevingsrisico's met betrekking tot communicatie