					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: P36S					Dokumenttitel: **Politik for sociale medier og ekstern kommunikation**						
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:						
X	Politik		Standard		Procedure		Formular		Register		Andet

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Tilpasset relevante standarder og regler

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 5.1, 5.2, 6.1, 8	Ledelse, risikostyring og operationel styring af ekstern kommunikation
ISO/IEC 27002:2022	Kontrol 5.10, 5.11	Acceptabel brug og informationssikkerhed i kommunikation
NIST SP 800-53 Rev.5	PL-4, AU-7, IR-6, AC-22	Adfærdsregler, revision, hændelsesrapportering samt styring af offentligt tilgængeligt indhold og adgang
EU GDPR	Artikel 5, 32, 33	Databeskyttelsesprincipper, behandlingssikkerhed og underretning ved brud med betydning for offentlig kommunikation
EU NIS2	Artikel 21(2)(e), 21(2)(f)	Politikker for systembrug og risikostyring i forsyningskæden og offentlig kommunikation
EU DORA	Artikel 14(4)	Kommunikationsforpligtelser efter hændelser

1. Formål

1.1. Denne politik fastsætter obligatoriske retningslinjer for al ekstern kommunikation, herunder brug af sociale medier, pressekontakt og eksternt digitalt indhold, når virksomheden, dens personale, klienter, systemer eller interne praksis omtales.

1.2. Politikken skal bidrage til at beskytte virksomhedens omdømme, sikre overholdelse af lovmæssige og regulatoriske krav samt reducere risikoen for informationslækage, misinformation og sikkerhedshændelser.

1.3. Politikken gør det muligt for medarbejdere og samarbejdspartnere at deltage positivt og ansvarligt i onlinediskussioner, samtidig med at utilsigtet offentliggørelse eller fejlagtig fremstilling undgås.

1.4. Politikken understøtter SME-beredskabet til ISO/IEC 27001-certificering ved at adressere styringen af oplysninger, der gøres tilgængelige for offentligheden eller eksterne interessenter.

2. Omfang

2.1. Denne politik gælder for alle personer med tilknytning til organisationen, herunder:

2.1.1. Medarbejdere og kontraktansatte

2.1.2. Freelancere, konsulenter og tredjepartsleverandører

2.1.3. Praktikanter eller deltidsansatte, der deltager i leverancer til kunder eller har systemadgang

2.2. Politikken gælder for alle former for ekstern kommunikation, der omtaler organisationen, herunder:

2.2.1. Opslag på sociale medier (LinkedIn, X/Twitter, TikTok, Instagram, Facebook osv.)

2.2.2. Blogindlæg, onlinefora, kundeanmeldelser og diskussionstråde

2.2.3. Oplæg eller deltagelse ved eksterne arrangementer (f.eks. konferencer, webinarer, podcasts)

2.2.4. E-mails eller beskeder til journalister, myndighedsrepræsentanter eller influencere

2.2.5. Offentligt delte skærmbilleder, fotos eller videoer fra arbejdsmiljøer

2.3. Politikken gælder også, når sådan kommunikation sker:

2.3.1. Fra personlige enheder eller konti

2.3.2. Uden for normal arbejdstid

2.3.3. Uden ondsindet hensigt; også utilsigtede eller spontant fremsatte bemærkninger er omfattet, hvis de omtaler virksomheden

3. Mål

3.1. Beskyttelse af omdømme: Forebygge skade på virksomhedens omdømme som følge af uautoriseret eller upassende offentlig kommunikation

3.2. Informationssikkerhed: Undgå utilsigtet eksponering af følsomme data, interne systemer eller klientoplysninger via sociale medier eller offentlige kanaler

3.3. Juridisk og regulatorisk overholdelse: Sikre, at alt offentligt indhold, der omtaler virksomheden, overholder gældende lovgivning om databeskyttelse og forretningskommunikation

3.4. Professionel adfærd: Fremme ansvarlig deltagelse i onlinediskussioner og mediekontakt, også fra personlige konti

3.5. Hændelsesberedskab: Sikre klare og operationelle handlingstrin ved utilsigtet offentliggørelse eller overtrædelser af politikken

4. Roller og ansvar

4.1. Direktør (GM)

4.1.1. Er ejer af og godkender denne politik

4.1.2. Gennemgår og godkender alle offentlige udtalelser, presseaktiviteter og medieinterviews

4.1.3. Sikrer, at denne politik kommunikeres tydeligt til alle medarbejdere og tredjeparter

4.1.4. Undersøger og håndterer alle overtrædelser af denne politik i koordinering med procedurerne for hændelseshåndtering

4.2. Udpeget medarbejder eller kommunikationsansvarlig (hvis udpeget)

4.2.1. Understøtter direktøren ved at gennemgå indhold før ekstern offentliggørelse (f.eks. blogindlæg eller emner til oplæg)

4.2.2. Vedligeholder log over godkendte medieaktiviteter eller opslag på sociale medier med høj risiko

4.2.3. Overvåger, i det omfang kapaciteten tillader det, kendte omtaler af virksomheden online med henblik på omdømme- eller sikkerhedsrisici

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Krav til gennemgang og opdatering

9.1. Årlig gennemgang

9.1.1. Denne politik skal gennemgås mindst én gang årligt af direktøren (GM)

9.1.2. Gennemgangen skal sikre overensstemmelse med opdaterede juridiske forpligtelser, udviklingstendenser inden for branchekommunikation og interne forretningsændringer

9.2. Udløsende forhold for gennemgang

9.2.1. Denne politik skal opdateres straks efter:

9.2.1.1. En væsentlig hændelse på sociale medier eller et omdømmemæssigt forhold

9.2.1.2. En ændring i tredjepartsleverandører, der håndterer kommunikation

9.2.1.3. Ny lovgivning eller nye regulatoriske forpligtelser vedrørende onlinekommunikation, medier eller branding

9.3. Dokumentation af ændringer

9.3.1. Alle opdateringer skal registreres, herunder revisionsdato, resumé af ændringer og direktørens godkendelse

9.3.2. Der skal opretholdes en versionshistorik til brug for revision og certificering

9.4. Distribution af opdateringer

9.4.1. Alle medarbejdere og kontraktansatte skal informeres om ændringer i politikken

9.4.2. Opdaterede versioner skal deles via e-mail eller interne portaler

9.4.3. Alle leverandører af offentlig kommunikation skal bekræfte opdaterede vilkår, før arbejdet fortsætter

10. Relaterede politikker og sammenhænge

10.1. Denne politik fungerer i sammenhæng med følgende SME-politikker:

10.1.1. P3S – Politik for acceptabel brug: Definerer acceptabel adfærd ved brug af kommunikationsplatforme, herunder adgang til sociale medier i arbejdstiden

10.1.2. P8S – Politik for informationssikkerhedsbevidsthed og uddannelse: Sikrer, at medarbejdere er uddannet til at identificere risici ved overdreven deling, phishing eller omdømmemæssige trusler online

10.1.3. P17S – Databeskyttelses- og privatlivspolitik: Sikrer, at personoplysninger og kundedata ikke deles i ekstern kommunikation i overensstemmelse med GDPR og andre juridiske krav

10.1.4. P30S – Politik for hændelseshåndtering: Regulerer håndteringen af utilsigtet offentliggørelse, onlinetrusler eller omdømmemæssige angreb som følge af misbrug af sociale medier

10.1.5. P37S – Politik for juridisk og regulatorisk overholdelse: Fastlægger organisationens bredere juridiske og kontraktuelle forpligtelser ved offentlig deling af indhold

10.2. Disse politikker skal anvendes samlet for at opretholde en sikker, respektfuld og juridisk compliant ekstern tilstedeværelse.

11. Referencestandarder og rammeværker

11.1. ISO/IEC 27001

11.1.1. Klausul 5.1 – Ledelse og forpligtelse: Kræver ledelsesmæssigt tilsyn med omdømmemæssige risici og informationsrisici

11.1.2. Klausul 6.1 – Risikostyring: Omfatter risici relateret til kommunikation

11.1.3. Klausul 8.1 – Operationel planlægning og styring: Omfatter regler for, hvordan oplysninger kommunikeres eksternt

11.2. ISO/IEC 27002

11.2.1. Kontrol 5.10 – Acceptabel brug af information og aktiver

11.2.2. Kontrol 5.11 – Informationssikkerhed i kommunikation

11.3. NIST SP 800-53 Rev. 5

11.3.1. PL-4 – Adfærdsregler: Regulerer passende adfærd ved brug af informationsressourcer

11.3.2. AU-7 – Revisionsreduktion og rapportgenerering: Understøtter overvågning af brugen af offentlige systemer

11.3.3. IR-6 – Hændelsesrapportering: Kræver respons på omdømmemæssige brud og kommunikationsrelaterede brud

11.3.4. AC-22 – Offentligt tilgængeligt indhold: Sikrer styring af eksterne publikationer og adgang

11.4. EU GDPR (2016/679)

11.4.1. Artikel 5 – Principper for behandling af personoplysninger (korrekthed, integritet, ansvarlighed)

11.4.2. Artikel 32 – Behandlingssikkerhed: Kræver sikkerhedsforanstaltninger omkring offentlig deling

11.4.3. Artikel 33 – Underretning ved brud: Udløses, hvis personoplysninger eksponeres via ekstern kommunikation

11.5. EU NIS2-direktivet (2022/2555)

11.5.1. Artikel 21(2)(e) – Politikker for brug af informationssystemer, herunder kommunikationsplatforme

11.5.2. Artikel 21(2)(f) – Politikker for håndtering af cybersikkerhedsrisici i forsyningskæden og på offentlige platforme

11.6. EU DORA (2022/2554)

11.6.1. Artikel 14(4) – Kommunikationsforpligtelser over for kunder, tredjeparter og myndigheder efter driftsmæssige hændelser

11.7. COBIT 2019

11.7.1. APO09 – Styring af serviceaftaler: Omfatter tilsyn med leverandører og kommunikationsrelaterede tredjeparter

11.7.2. DSS05 – Styring af sikkerhedstjenester: Omfatter beskyttelse af offentligt tilgængelige digitale aktiver

11.7.3. EDM03 – Sikring af risikooptimering: Fremhæver styring af omdømmemæssige risici og efterlevelsesrisici relateret til kommunikation