					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/forordning	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8	Definerede processer og rollebaseret styring for håndtering af offentlig kommunikation, som sikrer nøjagtighed, godkendelsesworkflow og eskalering af hændelser.
ISO/IEC 27002:2022	Kontroller 5.10, 5.11, 5.35, 5.36	Regulerer brug, acceptabel brug, kontakt med eksterne parter/myndigheder og rapportering af efterlevelse.
NIST SP 800-53 Rev.5	AC-8, AU-12, PL-4	Regler for brug af systemer og kommunikation, brugermeddelelser og opbevaring af revisionsspor.
EU GDPR	Artikler 5, 25, 32, 33	Principper for databehandling, databeskyttelse gennem design, behandlingssikkerhed og krav om underretning ved brud.
EU NIS2	Artikel 21	Foranstaltninger til styring af cybersikkerhedsrisici samt forpligtelser ved hændelser og risikorelateret offentlig kommunikation.
EU DORA	Artikler 9, 16	Styring af IKT-risici og kommunikationsstrategi for kritiske udbydere.
COBIT 2019	APO09, DSS05	Styring af serviceaftaler og kommunikation samt sikker kommunikationspraksis og hændelseshåndtering.

1. Formål

1.1 Denne politik fastsætter obligatoriske regler samt roller og ansvar for brug af sociale medier og alle former for ekstern kommunikation udført af personer med tilknytning til organisationen.

1.2 Den skal sikre, at offentlig kommunikation – uanset om den er planlagt eller spontan – er korrekt, respektfuld, sikker, lovmedholdelig og i overensstemmelse med organisationens brand.

1.3 Politikken har til formål at minimere risici forbundet med omdømmeskade, regulatoriske overtrædelser, lækage af immaterielle rettigheder og uautoriseret videregivelse via offentligt tilgængelige kanaler.

1.4 Politikken skal endvidere fremme ansvarlighed og struktureret styring i alle former for digital kommunikation, der involverer eller påvirker organisationen.

2. Omfang

2.1 Denne politik gælder for alle medarbejdere, kontraktansatte og tredjepartsleverandører, praktikanter og repræsentanter for tredjeparter, som:

2.1.1 Kommunikerer på vegne af organisationen, enten officielt eller uformelt

2.1.2 Refererer til eller giver indtryk af tilknytning til organisationen i offentlige sammenhænge

2.1.3 Bruger personlige eller virksomhedsrelaterede konti til at deltage i offentlige drøftelser, der involverer organisationen

2.2 Omfattede kommunikationskanaler omfatter, men er ikke begrænset til:

2.2.1 Sociale medieplatforme (f.eks. LinkedIn, X/Twitter, Instagram, TikTok, YouTube, Facebook)

2.2.2 Blogs, wikier, fora og offentlige debatplatforme

2.2.3 E-mail eller direkte beskeder til eksterne parter (f.eks. kunder, tilsynsmyndigheder, medier)

2.2.4 Presseinterviews, paneldebatter eller optagede medieoptrædener

2.2.5 Deltagelse i onlinefællesskaber, hvor organisationen omtales

2.3 Denne politik regulerer både kommunikation i realtid og forhåndsplanlagt indhold og gælder for alle enheder og konti (personlige eller virksomhedsrelaterede), der anvendes til at formidle kommunikationen.

3. Mål

3.1 At forhindre utilsigtet eller bevidst videregivelse af fortrolige, følsomme eller regulerede oplysninger via eksterne kommunikationskanaler.

3.2 At sikre, at officielle offentlige udtalelser og indhold på sociale medier er korrekte, autoriserede og i overensstemmelse med virksomhedens brand, etik og strategiske budskaber.

3.3 At forebygge omdømmeskade og sikre ensartet kommunikation på tværs af interne afdelinger og eksterne platforme.

3.4 At overholde gældende juridiske forpligtelser vedrørende offentlige udtalelser, herunder, men ikke begrænset til, GDPR, NIS2, DORA og sektorspecifikke regler for kommunikation.

3.5 At definere klare roller og ansvar, tilladte anvendelsestilfælde og håndhævelsesprotokoller for alt personale, der deltager i offentligt tilgængelige aktiviteter.

4. Roller og ansvar

4.1 Marketingdirektør, kommunikationsdirektør eller PR-ansvarlig

4.1.1 Godkender al officiel virksomhedskommunikation til ekstern offentliggørelse

4.1.2 Vedligeholder planer for indhold på sociale medier og retningslinjer for ensartet brandanvendelse

4.1.3 Overvåger onlineomtale og medieeksponering vedrørende organisationen

4.2 Chief Information Security Officer (CISO) / informationssikkerhedsteam

4.2.1 Overvåger digitale platforme for indikatorer på datalækage, identitetsmisbrug eller phishingforsøg

4.2.2 Koordinerer med hændelseshåndteringsteam ved angreb eller brud via sociale medier

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

9. Håndhævelse og efterlevelse

9.1 Denne politik er obligatorisk for alt omfattet personale og tredjeparter. Manglende efterlevelse kan medføre:

9.1.1 Formelle advarsler

9.1.2 Midlertidig eller permanent tilbagekaldelse af adgang til platforme eller systemer

9.1.3 Disciplinære foranstaltninger, herunder ophør af ansættelse eller engagement

9.1.4 Retssager, hvis ekstern kommunikation medfører omdømmeskade, brud på persondatasikkerheden eller manglende regulatorisk efterlevelse

9.2 Disciplinære foranstaltninger

9.2.1 Interne overtrædelser (f.eks. lækage af fortrolige data eller ærekrænkelse af organisationen) medfører involvering af HR, formel undersøgelse og dokumentation i medarbejderens personalesag.

9.2.2 Hvor relevant skal juridisk og compliance forfølge civilretlige retsmidler eller underrette myndigheder om strafbare forhold (f.eks. identitetsmisbrug eller lækage af intern viden).

9.3 Overvågning af efterlevelse

9.3.1 Sikkerhedsteamet og kommunikationsfunktionen skal udføre løbende overvågning af:

9.3.1.1 Omtaler af brandet på tværs af større platforme

9.3.1.2 Uofficiel brug af virksomhedens billeder eller varemærker

9.3.1.3 Kendte risici (f.eks. utilfredse medarbejdere eller forsøg på identitetsmisbrug)

9.3.2 Overvågningen skal ske i overensstemmelse med regler om medarbejderes databeskyttelse og privatliv, og alle markerede tilfælde skal verificeres ved manuel gennemgang.

9.4 Whistleblowerordning og rapportering af misbrug

9.4.1 Enhver medarbejder, der har mistanke om overtrædelse af denne politik, opfordres til at rapportere dette til informationssikkerhedsteamet, juridisk og compliance eller anonymt via whistleblowerportalen.

9.4.2 Gengældelse mod whistleblowere er strengt forbudt og medfører øjeblikkelig disciplinær handling.

10. Krav til gennemgang og opdatering

10.1 Denne politik skal gennemgås årligt eller tidligere, hvis:

10.1.1 Der sker væsentlige ændringer i regulatoriske krav (f.eks. nye EU-regler for digital kommunikation)

10.1.2 Nye sociale platforme eller kommunikationskanaler tages i brug

10.1.3 Der opstår en væsentlig hændelse eller gentagne overtrædelser, som indikerer mangler i processen

10.1.4 Der sker organisatoriske ændringer eller ledelsesændringer i PR-, juridiske eller sikkerhedsmæssige funktioner

10.2 Gennemgangen skal gennemføres i fællesskab af:

10.2.1 Marketingchefen / PR-ansvarlig

10.2.2 CISO eller ansvarlig for sikkerhedsrisici

10.2.3 Medarbejdere med ansvar for juridisk og compliance

10.3 Opdateringer skal dokumenteres i registeret over politikændringer og kommunikeres via interne awareness-kanaler. Ved væsentlige ændringer skal alt berørt personale afgive fornyet bekræftelse af politikken.

11. Relaterede politikker og sammenhænge

11.1 Denne politik understøttes af og hænger sammen med følgende komponenter i organisationens ledelsessystem for informationssikkerhed (ISMS):

11.1.1 P1 – Informationssikkerhedspolitik: Fastlægger overordnede principper for beskyttelse af oplysninger, herunder at kommunikation ikke må medføre uautoriseret videregivelse.

11.1.2 P3 – Politik for acceptabel brug: Definerer acceptable adfærdsmønstre for digitale platforme og teknologier, som direkte regulerer personlig og professionel brug af sociale kanaler.

11.1.3 P6 – Politik for risikostyring: Tilvejebringer styringsrammen for vurdering af trusler relateret til offentlig kommunikation og omdømmemæssig eksponering.

11.1.4 P8 – Politik for informationssikkerhedsbevidsthed og uddannelse: Fastlægger awareness-programmer, som uddanner medarbejdere i sikker kommunikationspraksis og trusler fra social engineering.

11.1.5 P13 – Politik for dataklassificering og mærkning: Vejleder personale i, hvad der udgør afskærmede eller fortrolige oplysninger, som ikke må videregives eksternt.

11.1.6 P30 – Politik for hændelseshåndtering: Definerer, hvordan kommunikationsrelaterede hændelser skal håndteres, herunder datalækager, identitetsmisbrug og regulatoriske overtrædelser.

11.1.7 P33 – Politik for revisions- og efterlevelsesovervågning: Regulerer de revisionsprocesser, der validerer kontroller for sociale medier, overvågningssystemer og efterlevelse af politikker for ekstern kommunikation.

12. Referencestandarder og rammeværker

12.1 ISO/IEC 27001:

12.1.1 Klausul 8.1 – operationel planlægning og styring: Kræver definerede processer og rollebaseret styring for håndtering af offentlig kommunikation, som sikrer nøjagtighed, godkendelsesworkflow og eskalering af hændelser med data- eller omdømmerisiko.

12.2 ISO/IEC 27002:2022:

12.2.1 Kontrol 5.10 – brug af information: Regulerer autoriseret og etisk formidling af intern eller ekstern kommunikation.

12.2.2 Kontrol 5.11 – acceptabel brug af information og aktiver: Understøtter acceptable praksisser for deling af indhold ved brug af virksomhedens aktiver eller personlige konti.

12.2.3 Kontrol 5.35 – kontakt med myndigheder: Kræver struktureret og autoriseret ekstern kommunikation med regulerende myndigheder og offentlige organer.

12.2.4 Kontrol 5.36 – overholdelse af politikker og standarder: Håndhæver konsekvent anvendelse af interne politikker i alle kommunikationsscenarier.

12.3 NIST SP 800-53 Rev.5:

12.3.1 PL-4 – adfærdsregler: Kræver formelle regler for brug af systemer og kommunikation, herunder standarder for offentlig videregivelse.

12.3.2 AC-8 – meddelelse om systembrug: Understøtter obligatoriske disclaimere og indholdsadvarsler på eksternt vendte platforme.

12.3.3 AU-12 – opbevaring af revisionsspor: Gælder for opbevaring af logfiler og kommunikationshistorik med henblik på hændelsesgennemgang og revision.

12.4 EU GDPR (2016/679):

12.4.1 Artikel 5 – principper for databehandling: Forbyder uautoriseret deling af personoplysninger via offentlig kommunikation.

12.4.2 Artikel 25 – databeskyttelse gennem design og standardindstillinger: Kræver indbygget databeskyttelse i kommunikationsværktøjer og workflow for indhold.

12.4.3 Artikel 32 – behandlingssikkerhed: Omfatter kryptering, adgangsstyring og processer for indholdsgodkendelse.

12.4.4 Artikel 33 – underretning ved brud: Kræver rettidig underretning om lækage af personoplysninger via offentlige kanaler.

12.5 EU NIS2-direktivet (2022/2555):

12.5.1 Artikel 21 – foranstaltninger til styring af cybersikkerhedsrisici: Omfatter kommunikationsprotokoller og forpligtelser under hændelser samt offentlig kommunikation om risici.

12.6 EU DORA (2022/2554):

12.6.1 Artikel 9 – styring af IKT-risici: Gælder for eksternt udløste kommunikationsrisici såsom identitetsmisbrug, misinformation og omdømmeforstyrrelser.

12.6.2 Artikel 16 – kommunikationsstrategi: Kræver, at kritiske finansielle virksomheder eller tjenesteudbydere styrer kommunikationsrisici og respons i krisescenarier.

12.7 COBIT 2019:

12.7.1 APO09 – Managed Service Agreements and Communication: Kræver struktureret styring af intern og ekstern kommunikation.

12.7.2 DSS05 – Manage Security Services: Sikrer, at kommunikationsaktiviteter ikke introducerer yderligere risiko eller underminerer processer for hændelseshåndtering.