					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P36S					Dokumenttitel: **Policy för sociala medier och extern kommunikation**							
Version: 1.0		Ikraftträdandedatum: 01.01.2025			Dokumentägare:							
X	Policy		Standard		Rutin		Formulär		Register		Övrigt	

Revisionshistorik				
Revisionsnummer	**Revisionsdatum**	**Ändringar**	**Granskad av**	**Processägare**

Godkännanden			
Namn	**Titel**	**Datum**	**Underskrift**

Ansluten till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8	Definierade processer och rollbaserad styrning för hantering av offentlig kommunikation för att säkerställa korrekthet, godkännandeflöden och eskalering av incidenter.
ISO/IEC 27002:2022	Kontrollerna 5.10, 5.11, 5.35, 5.36	Styr användning och godtagbar användning, extern kontakt och kommunikation med myndigheter samt rapportering av efterlevnad.
NIST SP 800-53 Rev.5	AC-8, AU-12, PL-4	Regler för användning av system och kommunikation, användaraviseringar samt bevarande av revisionsunderlag.
EU:s GDPR	Artiklarna 5, 25, 32, 33	Principer för behandling av personuppgifter, dataskydd genom teknik och dataskydd som standard, säkerhet i behandlingen samt krav på incidentanmälan.
EU:s NIS2-direktiv	Artikel 21	Åtgärder för cybersäkerhetsriskhantering samt skyldigheter vid incidenter och offentlig riskrelaterad kommunikation.
DORA-förordningen	Artiklarna 9, 16	IKT-riskhantering och kommunikationsstrategi för kritiska leverantörer.
COBIT 2019	APO09, DSS05	Styrning av tjänsteöverenskommelser och kommunikation samt säkra kommunikationsrutiner och incidenthantering.

1. Syfte

1.1 Denna policy fastställer bindande regler och ansvar för användning av sociala medier och all extern kommunikation av personal med anknytning till organisationen.

1.2 Den säkerställer att offentlig kommunikation, oavsett om den är planerad eller spontan, är korrekt, respektfull, säker, förenlig med tillämpliga lagkrav och konsekvent i förhållande till organisationens varumärke.

1.3 Policyn syftar till att minimera risker kopplade till anseendeskada, regelöverträdelser, exponering av immateriella rättigheter och obehörigt röjande via publika kanaler.

1.4 Policyn främjar även ansvarstagande och strukturerad styrning i all digital kommunikation som involverar eller påverkar organisationen.

2. Omfattning

2.1 Denna policy gäller för alla anställda, entreprenörer, tredjepartstjänsteleverantörer, praktikanter och tredjepartsrepresentanter som:

2.1.1 kommunicerar på organisationens vägnar, formellt eller informellt

2.1.2 hänvisar till eller antyder anknytning till organisationen i offentliga sammanhang

2.1.3 använder personliga eller organisatoriska konton för att delta i offentliga diskussioner som rör organisationen

2.2 Kommunikationskanaler som omfattas inkluderar, men är inte begränsade till:

2.2.1 plattformar för sociala medier (t.ex. LinkedIn, X/Twitter, Instagram, TikTok, YouTube, Facebook)

2.2.2 bloggar, wikis, forum och publika diskussionsforum

2.2.3 e-post eller direktmeddelanden till externa parter (t.ex. kunder, tillsynsmyndigheter, media)

2.2.4 pressintervjuer, paneldebatter eller inspelade medieframträdanden

2.2.5 deltagande i onlinegemenskaper där organisationen omnämns

2.3 Denna policy reglerar både realtidsinnehåll och schemalagt innehåll och gäller för alla enheter och konton, personliga eller organisatoriska, som används för att sprida kommunikationen.

3. Mål

3.1 Att förhindra oavsiktligt eller avsiktligt röjande av konfidentiell, känslig eller reglerad information via externa kommunikationskanaler.

3.2 Att säkerställa att officiella offentliga uttalanden och innehåll i sociala medier är korrekta, behörigen godkända och i linje med organisationens varumärke, etik och strategiska budskap.

3.3 Att förebygga anseendeskada och säkerställa konsekvent kommunikation mellan interna avdelningar och externa plattformar.

3.4 Att uppfylla tillämpliga rättsliga skyldigheter avseende offentliga uttalanden, inklusive men inte begränsat till GDPR, NIS2, DORA och sektorsspecifika regler för kommunikation.

3.5 Att fastställa tydliga ansvar, tillåtna användningsfall och tillämpningsrutiner för all personal som deltar i aktiviteter riktade till allmänheten.

4. Roller och ansvar

4.1 Marknadschef, kommunikationschef eller PR-ansvarig

4.1.1 godkänner all officiell företagskommunikation för extern publicering

4.1.2 upprätthåller innehållskalendrar för sociala medier och riktlinjer för konsekvent varumärkesanvändning

4.1.3 övervakar omnämnanden online och medieexponering som rör organisationen

4.2 informationssäkerhetschef (CISO) eller informationssäkerhetsteamet

4.2.1 övervakar digitala plattformar för indikatorer på dataläckage, identitetskapning eller nätfiskeförsök

4.2.2 samordnar med incidenthanteringsteam vid attacker eller överträdelser via sociala medier

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Efterlevnad och tillämpning

9.1 Denna policy är bindande för all berörd personal och tredje part. Underlåtenhet att följa policyn kan leda till:

9.1.1 formella varningar

9.1.2 tillfällig eller permanent återkallelse av åtkomst till plattformar eller system

9.1.3 disciplinära åtgärder, inklusive avslut av anställning eller uppdrag

9.1.4 rättsliga åtgärder om extern kommunikation leder till anseendeskada, personuppgiftsincident eller bristande regulatorisk efterlevnad

9.2 Disciplinära åtgärder

9.2.1 Interna överträdelser (t.ex. läckage av konfidentiella uppgifter eller förtal av organisationen) ska leda till involvering av HR, formell utredning och dokumentation i personalakten.

9.2.2 När det är tillämpligt ska juridikfunktionen driva civilrättsliga åtgärder eller underrätta myndigheter om brottslig verksamhet (t.ex. identitetskapning eller läckor av insiderinformation).

9.3 Uppföljning av efterlevnad

9.3.1 Säkerhetsfunktionen och kommunikationsfunktionen ska utföra löpande övervakning av:

9.3.1.1 omnämnanden av varumärket på större plattformar

9.3.1.2 inofficiell användning av företagets bildmaterial eller varumärken

9.3.1.3 kända risker (t.ex. missnöjda anställda eller försök till identitetskapning)

9.3.2 Övervakning ska ske i enlighet med tillämpliga lagar och regler om anställdas integritet, och alla flaggade fall ska verifieras genom manuell granskning.

9.4 Visselblåsning och rapportering av missbruk

9.4.1 Alla anställda som misstänker en överträdelse av denna policy ska rapportera detta till informationssäkerhetsteamet, juridikfunktionen eller anonymt via visselblåsarkanalen.

9.4.2 Repressalier mot visselblåsare är strängt förbjudna och ska leda till omedelbara disciplinära åtgärder.

10. Krav för granskning och uppdatering

10.1 Denna policy ska granskas årligen, eller tidigare om:

10.1.1 det sker väsentliga förändringar i regulatoriska krav (t.ex. ny EU-lagstiftning om digital kommunikation)

10.1.2 nya sociala plattformar eller kommunikationskanaler införs

10.1.3 en betydande incident eller upprepade överträdelser indikerar processbrister

10.1.4 det sker förändringar i struktur eller ledning inom PR-, juridik- eller säkerhetsfunktionerna

10.2 Granskningen ska genomföras gemensamt av:

10.2.1 chef för marknad eller PR

10.2.2 CISO eller ansvarig för säkerhetsrisker

10.2.3 juridik- och complianceansvariga

10.3 Uppdateringar ska dokumenteras i registret för policyändringar och kommuniceras via interna kanaler för informationssäkerhetsmedvetenhet. Vid väsentliga ändringar ska all berörd personal bekräfta policyn på nytt.

11. Relaterade policyer och kopplingar

11.1 Denna policy stöds av och samverkar med följande delar av organisationens ledningssystem för informationssäkerhet (LIS):

11.1.1 P1 – Informationssäkerhetspolicy: Fastställer övergripande principer för att skydda information, inklusive att säkerställa att kommunikation inte leder till obehörigt röjande.

11.1.2 P3 – Policy för godtagbar användning: Definierar godtagbara beteenden för digitala plattformar och tekniker, vilket direkt reglerar personlig och professionell användning av sociala kanaler.

11.1.3 P6 – Riskhanteringspolicy: Tillhandahåller riskramverket för att bedöma hot relaterade till offentlig kommunikation och exponering för anseenderisker.

11.1.4 P8 – Policy för informationssäkerhetsmedvetenhet och utbildning: Ställer krav på medvetenhetsprogram som utbildar personal i säkra kommunikationsrutiner och hot från social manipulation.

11.1.5 P13 – Policy för dataklassificering och märkning: Vägleder personal om vad som utgör begränsad eller konfidentiell information som inte får röjas externt.

11.1.6 P30 – Policy för incidenthantering: Definierar hur incidenter relaterade till offentlig kommunikation ska hanteras, inklusive dataläckage, identitetskapning och regulatoriska överträdelser.

11.1.7 P33 – Policy för revisions- och efterlevnadsövervakning: Styr revisionsprocesser som validerar kontroller för sociala medier, övervakningssystem och efterlevnad av policyer för extern kommunikation.

12. Referensstandarder och ramverk

12.1 ISO/IEC 27001:

12.1.1 Klausul 8.1 – operativ planering och styrning: Kräver definierade processer och rollbaserad styrning för hantering av offentlig kommunikation för att säkerställa korrekthet, godkännandeflöden och eskalering av incidenter som rör data eller anseenderisk.

12.2 ISO/IEC 27002:2022:

12.2.1 Kontroll 5.10 – användning av information: Reglerar behörig och etisk spridning av intern eller extern kommunikation.

12.2.2 Kontroll 5.11 – godtagbar användning av information och andra tillgångar: Förstärker godtagbara arbetssätt för delning av innehåll med organisationens tillgångar eller via personliga konton.

12.2.3 Kontroll 5.35 – kontakt med myndigheter: Kräver strukturerad och behörig extern kommunikation med tillsynsmyndigheter och offentliga organ.

12.2.4 Kontroll 5.36 – efterlevnad av policyer, regler och standarder för informationssäkerhet: Säkerställer konsekvent tillämpning av interna policyer i alla kommunikationssituationer.

12.3 NIST SP 800-53 Rev.5:

12.3.1 PL-4 – beteenderegler: Kräver formella regler för användning av system och kommunikation, inklusive standarder för offentliggörande.

12.3.2 AC-8 – avisering om systemanvändning: Stödjer krav på ansvarsfriskrivningar och innehållsvarningar på externt riktade plattformar.

12.3.3 AU-12 – bevarande av revisionsunderlag: Gäller bevarande av loggar och kommunikationshistorik för incidentgranskning och revisionsändamål.

12.4 EU:s GDPR (2016/679):

12.4.1 Artikel 5 – principer för behandling av personuppgifter: Förbjuder obehörig delning av personuppgifter genom offentlig kommunikation.

12.4.2 Artikel 25 – dataskydd genom teknik och dataskydd som standard: Kräver dataskyddsåtgärder i kommunikationsverktyg och arbetsflöden för innehåll.

12.4.3 Artikel 32 – säkerhet i behandlingen: Omfattar kryptering, åtkomstkontroll och processer för godkännande av innehåll.

12.4.4 Artikel 33 – incidentanmälan: Kräver skyndsam anmälan av personuppgiftsincidenter via publika kanaler.

12.5 EU:s NIS2-direktiv (2022/2555):

12.5.1 Artikel 21 – åtgärder för cybersäkerhetsriskhantering: Omfattar kommunikationsprotokoll samt skyldigheter vid incidenter och offentlig riskkommunikation.

12.6 DORA-förordningen (2022/2554):

12.6.1 Artikel 9 – IKT-riskhantering: Gäller externt utlöst kommunikationsrisk såsom identitetskapning, desinformation och störningar med påverkan på anseendet.

12.6.2 Artikel 16 – kommunikationsstrategi: Kräver att kritiska finansiella entiteter eller tjänsteleverantörer hanterar kommunikationsrisker och respons i krissituationer.

12.7 COBIT 2019:

12.7.1 APO09 – Hantera tjänsteöverenskommelser och kommunikation: Kräver strukturerad styrning av intern och extern kommunikation.

12.7.2 DSS05 – Hantera säkerhetstjänster: Säkerställer att kommunikationsaktiviteter inte introducerar ytterligare risk eller undergräver incidenthanteringsprocesser.