					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**

Anslutning till standarder och regelverk där tillämpligt

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 5.1, 5.2, 6.1, 8	Ledarskap, riskhantering och operativ styrning av extern kommunikation
ISO/IEC 27002:2022	Kontroller 5.10, 5.11	Godtagbar användning och informationssäkerhet i kommunikation
NIST SP 800-53 Rev. 5	PL-4, AU-7, IR-6, AC-22	Beteenderegler, revision, incidentrapportering samt hantering av publikt innehåll och åtkomst
EU:s dataskyddsförordning (GDPR)	Artikel 5, 32, 33	Dataskyddsprinciper, säkerhet och anmälan av incidenter som påverkar offentlig kommunikation
EU:s NIS2-direktiv	Artikel 21.2 e, 21.2 f	Policyer för användning av system samt riskhantering i leveranskedjan och offentlig kommunikation
EU:s DORA-förordning	Artikel 14.4	Kommunikationsskyldigheter efter incidenter

1. Syfte

1.1. Denna policy fastställer bindande regler för all extern kommunikation riktad till allmänheten, inklusive användning av sociala medier, kontakter med press samt externt digitalt innehåll, när organisationen, dess personal, kunder, system eller interna arbetssätt omnämns.

1.2. Policyn ska bidra till att skydda organisationens anseende, upprätthålla efterlevnad av rättsliga och regulatoriska krav samt minska risken för informationsläckage, felaktig information och säkerhetsincidenter.

1.3. Policyn ska möjliggöra för personal och samarbetspartner att delta på ett positivt och ansvarsfullt sätt i diskussioner online, samtidigt som oavsiktliga röjanden och missvisande framställningar undviks.

1.4. Policyn stärker SME:s beredskap för certifiering enligt ISO/IEC 27001 genom att reglera styrningen av information som görs tillgänglig för allmänheten eller externa intressenter.

2. Omfattning

2.1. Denna policy gäller för alla personer som är knutna till organisationen, inklusive:

2.1.1. anställda och uppdragstagare

2.1.2. frilansare, konsulter och tredjepartsleverantörer

2.1.3. praktikanter och deltidsanställda som medverkar i kundleveranser eller har systemåtkomst

2.2. Policyn gäller för alla former av extern kommunikation som hänvisar till organisationen, inklusive:

2.2.1. inlägg i sociala medier (LinkedIn, X/Twitter, TikTok, Instagram, Facebook etc.)

2.2.2. blogginlägg, onlineforum, kundomdömen och diskussionstrådar

2.2.3. externa framträdanden (t.ex. konferenser, webbinarier, poddar)

2.2.4. e-post eller meddelanden till journalister, myndighetsföreträdare eller influerare

2.2.5. offentligt delade skärmbilder, fotografier eller videor från arbetsmiljöer

2.3. Policyn gäller även när sådan kommunikation sker:

2.3.1. från personliga enheter eller konton

2.3.2. utanför ordinarie arbetstid

2.3.3. utan skadligt uppsåt – även oavsiktliga eller i förbifarten lämnade kommentarer omfattas om de hänvisar till organisationen

3. Mål

3.1. Skydd av anseende: Förhindra skada på organisationens anseende genom obehörig eller olämplig offentlig kommunikation.

3.2. Informationssäkerhet: Förhindra oavsiktlig exponering av känsliga uppgifter, interna system eller kundinformation via sociala medier eller offentliga kanaler.

3.3. Efterlevnad av rättsliga och regulatoriska krav: Säkerställa att allt offentligt innehåll som hänvisar till organisationen uppfyller tillämpliga lagkrav avseende dataskydd och affärskommunikation.

3.4. Professionellt uppträdande: Främja ett ansvarsfullt deltagande i diskussioner online och mediekontakter, även via personliga konton.

3.5. Incidentberedskap: Tillhandahålla tydliga och praktiskt tillämpbara åtgärder vid oavsiktliga röjanden eller policyöverträdelser.

4. Roller och ansvar

4.1. Verkställande chef (GM)

4.1.1. äger och godkänner denna policy

4.1.2. granskar och godkänner uttalanden riktade till allmänheten, presskontakter och medieintervjuer

4.1.3. säkerställer att denna policy kommuniceras tydligt till alla anställda och tredje parter

4.1.4. utreder och hanterar överträdelser av denna policy i samordning med incidenthanteringsprocessen

4.2. Utsedd medarbetare eller kommunikationsansvarig (om sådan har utsetts)

4.2.1. stödjer GM genom att granska innehåll före extern publicering, exempelvis blogginlägg eller ämnen för föredrag

4.2.2. upprätthåller loggar över godkända medieaktiviteter eller inlägg i sociala medier med hög risk

4.2.3. övervakar, i den utsträckning resurser finns, kända omnämnanden av organisationen online avseende anseenderisker eller säkerhetsrisker

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

9. Krav för granskning och uppdatering

9.1. Årlig granskning

9.1.1. Denna policy ska granskas minst en gång per år av verkställande chef (GM)

9.1.2. Granskningen ska säkerställa anpassning till uppdaterade rättsliga skyldigheter, trender inom branschkommunikation och interna verksamhetsförändringar

9.2. Händelsestyrda granskningar

9.2.1. Denna policy ska uppdateras omedelbart efter:

9.2.1.1. en betydande incident i sociala medier eller ett anseenderelaterat problem

9.2.1.2. en förändring av tredjepartsleverantörer som hanterar kommunikation

9.2.1.3. ny lagstiftning eller nya regulatoriska skyldigheter som rör onlinekommunikation, medier eller varumärkesanvändning

9.3. Dokumentation av ändringar

9.3.1. Alla uppdateringar ska registreras, inklusive datum för revidering, ändringssammanfattning och godkännande av GM

9.3.2. En versionshistorik ska bevaras för revision och certifiering

9.4. Distribution av uppdateringar

9.4.1. All personal och alla uppdragstagare ska informeras om varje policyändring

9.4.2. Uppdaterade versioner ska distribueras via e-post eller interna portaler

9.4.3. Leverantörer som hanterar offentlig kommunikation ska bekräfta uppdaterade villkor innan arbetet fortsätter

10. Relaterade policyer och kopplingar

10.1. Denna policy ska tillämpas tillsammans med följande SME-policyer:

10.1.1. P3S – Policy för godtagbar användning: Definierar godtagbart beteende vid användning av kommunikationsplattformar, inklusive åtkomst till sociala medier under arbetstid

10.1.2. P8S – Policy för informationssäkerhetsmedvetenhet och utbildning: Säkerställer att personal utbildas i att identifiera risker kopplade till överdriven delning, nätfiske eller anseenderelaterade hot online

10.1.3. P17S – Policy för dataskydd och integritet: Säkerställer att personuppgifter och kunddata inte delas i extern kommunikation, i linje med GDPR och andra rättsliga krav

10.1.4. P30S – Policy för incidenthantering: Reglerar hanteringen av oavsiktligt offentligt röjande, onlinehot eller anseenderelaterade angrepp till följd av felaktig användning av sociala medier

10.1.5. P37S – Policy för rättslig och regulatorisk efterlevnad: Fastställer organisationens övergripande rättsliga och avtalsmässiga skyldigheter vid offentlig delning av innehåll

10.2. Dessa policyer ska tillämpas tillsammans för att upprätthålla en säker, respektfull och rättsenlig extern närvaro.

11. Referensstandarder och ramverk

11.1. ISO/IEC 27001

11.1.1. Klausul 5.1 – Ledarskap och åtagande: Kräver ledningens tillsyn över anseenderisker och informationsrisker

11.1.2. Klausul 6.1 – Riskhantering: Omfattar riskexponeringar kopplade till kommunikation

11.1.3. Klausul 8.1 – Operativ styrning: Omfattar regler för hur information kommuniceras externt

11.2. ISO/IEC 27002

11.2.1. Kontroll 5.10 – Godtagbar användning av information och tillgångar

11.2.2. Kontroll 5.11 – Informationssäkerhet i kommunikation

11.3. NIST SP 800-53 Rev. 5

11.3.1. PL-4 – Beteenderegler: Reglerar lämpligt uppträdande vid användning av informationsresurser

11.3.2. AU-7 – Reduktion av revisionsdata och generering av rapporter: Stödjer övervakning av offentlig systemanvändning

11.3.3. IR-6 – Incidentrapportering: Säkerställer respons på anseenderelaterade incidenter och kommunikationsöverträdelser

11.3.4. AC-22 – Publikt tillgängligt innehåll: Säkerställer kontroll över externa publikationer och åtkomst

11.4. EU:s dataskyddsförordning (GDPR) (2016/679)

11.4.1. Artikel 5 – Principer för behandling av personuppgifter (korrekthet, riktighet, ansvarsskyldighet)

11.4.2. Artikel 32 – Säkerhet i behandlingen: Kräver skyddsåtgärder vid offentlig delning

11.4.3. Artikel 33 – Anmälan av personuppgiftsincident: Aktiveras om personuppgifter exponeras genom extern kommunikation

11.5. EU:s NIS2-direktiv (2022/2555)

11.5.1. Artikel 21(2)(e) – Policyer för användning av informationssystem, inklusive kommunikationsplattformar

11.5.2. Artikel 21(2)(f) – Policyer för hantering av cybersäkerhetsrisker i leveranskedjan och på publika plattformar

11.6. EU:s DORA-förordning (2022/2554)

11.6.1. Artikel 14(4) – Kommunikationsskyldigheter gentemot kunder, tredje parter och myndigheter efter operativa incidenter

11.7. COBIT 2019

11.7.1. APO09 – Hantera tjänsteöverenskommelser: Omfattar tillsyn över leverantörer och tredje parter relaterade till kommunikation

11.7.2. DSS05 – Hantera säkerhetstjänster: Omfattar skydd av digitala tillgångar riktade till allmänheten

11.7.3. EDM03 – Säkerställ riskoptimering: Betonar hantering av anseenderisker och regelefterlevnadsrisker kopplade till kommunikation