					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P36S					Titolo del documento: **Politica sui social media e sulle comunicazioni esterne**							
Versione: 1.0		Data di entrata in vigore: 01.01.2025			Proprietario del documento:							
X	Politica		Standard		Procedura		Modulo		Registro		Altro	

Cronologia delle revisioni				
Numero di revisione	**Data di revisione**	**Modifiche**	**Riesaminato da**	**Proprietario del processo**

Approvazioni			
Nome	**Ruolo**	**Data**	**Firma**

Allineata a norme e regolamenti

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 8	Processi definiti e governance basata sui ruoli per la gestione delle comunicazioni pubbliche, al fine di garantire accuratezza, flussi di approvazione ed escalation degli incidenti.
ISO/IEC 27002:2022	Controls 5.10, 5.11, 5.35, 5.36	Disciplina l'uso delle informazioni, l'uso accettabile degli asset aziendali, i contatti esterni e con le autorità e la reportistica di conformità.
NIST SP 800-53 Rev.5	AC-8, AU-12, PL-4	Regole per l'uso dei sistemi e delle comunicazioni, notifiche agli utenti e conservazione dei log di audit.
EU GDPR	Articles 5, 25, 32, 33	Principi del trattamento dei dati, protezione dei dati fin dalla progettazione, sicurezza del trattamento e obblighi di notifica delle violazioni.
EU NIS2	Article 21	Misure di gestione dei rischi di cibersicurezza, obblighi in caso di incidenti e comunicazioni pubbliche relative al rischio.
EU DORA	Articles 9, 16	Gestione del rischio ICT e strategia di comunicazione per i fornitori critici.
COBIT 2019	APO09, DSS05	Governance degli accordi di servizio e delle comunicazioni, nonché pratiche di comunicazione sicura e gestione degli incidenti.

Finalità

1.1 La presente politica stabilisce regole e responsabilità obbligatorie che disciplinano l'utilizzo dei social media e di tutte le forme di comunicazione esterna da parte del personale affiliato all'organizzazione.

1.2 Garantisce che i messaggi pubblici, pianificati o estemporanei, siano accurati, rispettosi, sicuri, conformi ai requisiti di legge e coerenti con il marchio aziendale.

1.3 La politica mira a ridurre al minimo i rischi associati a danni reputazionali, violazioni normative, divulgazione di proprietà intellettuale e divulgazioni non autorizzate attraverso canali esposti pubblicamente.

1.4 La politica promuove inoltre responsabilizzazione e governance strutturata in tutte le forme di comunicazione digitale che coinvolgono o incidono sull'organizzazione.

2. Ambito di applicazione

2.1 La presente politica si applica a tutti i dipendenti, collaboratori esterni, tirocinanti e rappresentanti di terze parti che:

2.1.1 Comunicano per conto dell'organizzazione, in modo ufficiale o informale

2.1.2 Fanno riferimento all'organizzazione o lasciano intendere un'affiliazione con essa in un contesto pubblico

2.1.3 Utilizzano account personali o aziendali per partecipare a discussioni pubbliche che coinvolgono l'organizzazione

2.2 I canali di comunicazione coperti includono, a titolo esemplificativo e non esaustivo:

2.2.1 Piattaforme di social media (ad es. LinkedIn, X/Twitter, Instagram, TikTok, YouTube, Facebook)

2.2.2 Blog, wiki, forum e bacheche di discussione pubbliche

2.2.3 E-mail o messaggistica diretta verso parti esterne (ad es. clienti, autorità di regolamentazione, media)

2.2.4 Interviste alla stampa, tavole rotonde o apparizioni su media registrati

2.2.5 Partecipazione a comunità online in cui si fa riferimento all'organizzazione

2.3 La presente politica disciplina sia i contenuti pubblicati in tempo reale sia quelli programmati in anticipo e si applica a tutti i dispositivi e account, personali o aziendali, utilizzati per diffondere la comunicazione.

3. Obiettivi

3.1 Prevenire la divulgazione accidentale o intenzionale di informazioni riservate, sensibili o soggette a regolamentazione attraverso canali di comunicazione esterna.

3.2 Garantire che le dichiarazioni pubbliche ufficiali e i contenuti sui social media siano accurati, autorizzati e allineati all'identità del marchio aziendale, ai principi etici e ai messaggi strategici.

3.3 Prevenire danni reputazionali e garantire coerenza dei messaggi tra i dipartimenti interni e le piattaforme esterne.

3.4 Rispettare gli obblighi di legge applicabili relativi alle dichiarazioni pubbliche, inclusi, a titolo esemplificativo e non esaustivo, GDPR, NIS2, DORA e le regole di comunicazione specifiche di settore.

3.5 Definire con chiarezza responsabilità, casi d'uso consentiti e protocolli di applicazione della politica per tutto il personale coinvolto in attività esposte al pubblico.

4. Ruoli e responsabilità

4.1 Direttore Marketing o Comunicazione / Responsabile delle Relazioni Pubbliche

4.1.1 Approva tutti i messaggi ufficiali dell'azienda destinati alla pubblicazione esterna

4.1.2 Mantiene i calendari dei contenuti sui social media e le linee guida per la coerenza del marchio

4.1.3 Monitora le menzioni online e l'esposizione mediatica che coinvolgono l'organizzazione

4.2 Responsabile della sicurezza delle informazioni (CISO) / Team di sicurezza

4.2.1 Monitora le piattaforme digitali per individuare indicatori di perdita di dati, impersonificazione o tentativi di phishing

4.2.2 Si coordina con i team di risposta agli incidenti in caso di attacchi o violazioni tramite social media

[... Le sezioni 4.3–8 non sono incluse in questa anteprima. Acquistare il documento completo per accedere all'intero contenuto. ...]

9. Applicazione e conformità

9.1 La presente politica è obbligatoria per tutto il personale interessato e per le terze parti. Il mancato rispetto può comportare:

9.1.1 Avvertimenti formali

9.1.2 Revoca temporanea o permanente degli accessi alle piattaforme o ai sistemi

9.1.3 Misure disciplinari, inclusa la cessazione del rapporto

9.1.4 Azioni legali, se la comunicazione esterna determina danni reputazionali, violazione dei dati o non conformità normativa

9.2 Misure disciplinari

9.2.1 Le violazioni interne, ad esempio divulgazione di dati riservati o diffamazione dell'organizzazione, comportano il coinvolgimento delle Risorse Umane (HR), un'indagine formale e la relativa documentazione nel fascicolo del dipendente.

9.2.2 Ove applicabile, la Funzione Legale promuove rimedi civilistici o informa le autorità in caso di attività criminali, ad esempio impersonificazione o divulgazioni relative a insider trading.

9.3 Monitoraggio della conformità

9.3.1 I team Sicurezza e Comunicazione devono svolgere un monitoraggio continuo di:

9.3.1.1 Menzioni del marchio sulle principali piattaforme

9.3.1.2 Uso non ufficiale di immagini aziendali o marchi

9.3.1.3 Rischi noti, ad esempio dipendenti scontenti o tentativi di impersonificazione

9.3.2 Il monitoraggio deve rispettare le leggi e i regolamenti in materia di privacy dei dipendenti e tutti i casi segnalati devono essere verificati da un revisore umano.

9.4 Sistema di whistleblowing e segnalazione di usi impropri

9.4.1 Qualsiasi dipendente che sospetti una violazione della presente politica è incoraggiato a segnalarla al Team di sicurezza delle informazioni, alla Funzione Legale o in forma anonima tramite il portale di whistleblowing.

9.4.2 Qualsiasi ritorsione nei confronti dei segnalanti è severamente vietata e comporta immediata azione disciplinare.

10. Requisiti di riesame e aggiornamento

10.1 La presente politica deve essere riesaminata annualmente, o prima se:

10.1.1 Intervengono modifiche significative dei requisiti normativi, ad esempio nuove norme UE sulle comunicazioni digitali

10.1.2 Vengono adottate nuove piattaforme social o nuovi canali di comunicazione

10.1.3 Si verifica un incidente significativo o violazioni ripetute che evidenziano lacune nei processi

10.1.4 Si verifica un cambiamento strutturale o di leadership nelle funzioni PR, Legale o Sicurezza

10.2 Il riesame deve essere condotto congiuntamente da:

10.2.1 Il Responsabile Marketing / Relazioni Pubbliche

10.2.2 Il CISO o il responsabile del rischio di sicurezza

10.2.3 I Responsabili Affari Legali e Compliance

10.3 Gli aggiornamenti devono essere documentati nel Registro delle modifiche alle politiche e comunicati attraverso i canali interni di sensibilizzazione. In caso di modifiche sostanziali, tutto il personale interessato deve confermare nuovamente la presa visione della politica.

11. Politiche correlate e collegamenti

11.1 La presente politica è supportata dai seguenti componenti del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) dell'organizzazione ed è con essi interrelata:

11.1.1 P1 – Politica per la sicurezza delle informazioni: stabilisce i principi generali per la protezione delle informazioni, inclusa la necessità di garantire che le comunicazioni non comportino divulgazioni non autorizzate.

11.1.2 P3 – Politica di uso accettabile: definisce i comportamenti accettabili per piattaforme e tecnologie digitali e disciplina direttamente l'uso personale e professionale dei canali social.

11.1.3 P6 – Politica di gestione del rischio: fornisce il quadro di riferimento per la valutazione delle minacce connesse alla comunicazione pubblica e all'esposizione reputazionale.

11.1.4 P8 – Politica di consapevolezza e formazione sulla sicurezza delle informazioni: impone programmi di sensibilizzazione che istruiscono il personale sulle pratiche di comunicazione sicura e sulle minacce di ingegneria sociale.

11.1.5 P13 – Politica di classificazione ed etichettatura dei dati: guida il personale nell'identificazione delle informazioni riservate o soggette a restrizioni che non devono essere divulgate all'esterno.

11.1.6 P30 – Politica di risposta agli incidenti (P30): definisce le modalità di gestione degli incidenti connessi alle comunicazioni pubbliche, comprese perdite di dati, impersonificazione e violazioni normative.

11.1.7 P33 – Politica di monitoraggio dell'audit e della conformità: disciplina i processi di audit che convalidano i controlli sui social media, i sistemi di monitoraggio e la conformità alle politiche di comunicazione esterna.

12. Standard e quadri di riferimento

12.1 ISO/IEC 27001:

12.1.1 Clause 8.1 – Pianificazione operativa e controllo: richiede processi definiti e governance basata sui ruoli per la gestione delle comunicazioni pubbliche, al fine di garantire accuratezza, flussi di approvazione ed escalation degli incidenti che comportano rischi per i dati o la reputazione.

12.2 ISO/IEC 27002:2022:

12.2.1 Controllo 5.10 – Uso delle informazioni: disciplina la diffusione autorizzata ed etica delle comunicazioni interne o esterne.

12.2.2 Controllo 5.11 – Uso accettabile delle informazioni e degli asset: rafforza le pratiche accettabili per la condivisione di contenuti mediante asset aziendali o account personali.

12.2.3 Controllo 5.35 – Contatti con le autorità: richiede comunicazioni esterne strutturate e autorizzate con autorità di regolamentazione ed enti pubblici.

12.2.4 Controllo 5.36 – Conformità a politiche e norme: richiede l'applicazione coerente delle politiche interne in tutti gli scenari di comunicazione.

12.3 NIST SP 800-53 Rev.5:

12.3.1 PL-4 – Regole di comportamento: richiede regole formali per l'uso dei sistemi e delle comunicazioni, inclusi standard per la divulgazione pubblica.

12.3.2 AC-8 – Notifica sull'uso del sistema: supporta l'uso obbligatorio di disclaimer e avvertenze sui contenuti nelle piattaforme esposte verso l'esterno.

12.3.3 AU-12 – Conservazione delle registrazioni di audit: si applica alla conservazione dei log e della cronologia delle comunicazioni ai fini del riesame degli incidenti e dell'audit.

12.4 GDPR UE (2016/679):

12.4.1 Articolo 5 – Principi del trattamento dei dati: vieta la condivisione non autorizzata di dati personali attraverso comunicazioni pubbliche.

12.4.2 Articolo 25 – Protezione dei dati fin dalla progettazione e per impostazione predefinita: richiede misure di tutela della privacy negli strumenti di comunicazione e nei flussi di lavoro dei contenuti.

12.4.3 Articolo 32 – Sicurezza del trattamento: si applica ai processi di cifratura, controllo degli accessi e approvazione dei contenuti.

12.4.4 Articolo 33 – Notifica della violazione: impone la comunicazione tempestiva delle violazioni dei dati personali tramite canali pubblici.

12.5 Direttiva UE NIS2 (2022/2555):

12.5.1 Articolo 21 – Misure di gestione dei rischi di cibersicurezza: include protocolli di comunicazione e obblighi in caso di incidenti e comunicazioni pubbliche relative al rischio.

12.6 DORA UE (2022/2554):

12.6.1 Articolo 9 – Gestione del rischio ICT: si applica ai rischi di comunicazione attivati dall'esterno, quali impersonificazione, disinformazione e turbative reputazionali.

12.6.2 Articolo 16 – Strategia di comunicazione: richiede che i fornitori critici di servizi finanziari o di servizi gestiscano i rischi di comunicazione e le relative risposte negli scenari di crisi.

12.7 COBIT 2019:

12.7.1 APO09 – Managed Service Agreements and Communication: richiede governance strutturata sulle comunicazioni interne ed esterne.

12.7.2 DSS05 – Gestire i servizi di sicurezza: garantisce che le attività di comunicazione non introducano rischi aggiuntivi né compromettano i processi di gestione degli incidenti.