					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**

Allineamento a norme e regolamenti

Norma/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausole 5.1, 5.2, 6.1, 8	Leadership, gestione del rischio e controllo operativo delle comunicazioni esterne
ISO/IEC 27002:2022	Controlli 5.10, 5.11	Uso accettabile e sicurezza delle informazioni nelle comunicazioni
NIST SP 800-53 Rev.5	PL-4, AU-7, IR-6, AC-22	Regole di comportamento, audit, segnalazione degli incidenti e gestione dei contenuti e degli accessi pubblici
GDPR UE	Articoli 5, 32, 33	Principi di protezione dei dati, sicurezza e notifica delle violazioni con impatto sulle comunicazioni pubbliche
NIS2 UE	Articolo 21(2)(e), 21(2)(f)	Politiche per l'uso dei sistemi e gestione dei rischi della catena di fornitura e delle comunicazioni pubbliche
DORA UE	Articolo 14(4)	Obblighi di comunicazione a seguito di incidenti

1. Finalità

1.1. La presente politica stabilisce linee guida vincolanti per tutte le comunicazioni rivolte al pubblico, compreso l'uso dei social media, i rapporti con la stampa e i contenuti digitali esterni, quando fanno riferimento all'azienda, al suo personale, ai clienti, ai sistemi o alle prassi interne.

1.2. La politica contribuisce a tutelare la reputazione dell'azienda, mantenere la conformità legale e regolamentare e ridurre il rischio di perdita di dati, disinformazione o incidenti di sicurezza.

1.3. La politica consente al personale e ai partner di partecipare in modo positivo e responsabile alle discussioni online, prevenendo al contempo divulgazioni accidentali o rappresentazioni non corrette.

1.4. La politica rafforza la preparazione della PMI alla certificazione ISO/IEC 27001 disciplinando il controllo delle informazioni rese disponibili al pubblico o a soggetti esterni interessati.

2. Ambito di applicazione

2.1. La presente politica si applica a tutti i soggetti affiliati all'organizzazione, inclusi:

2.1.1. dipendenti e collaboratori esterni

2.1.2. freelance, consulenti e fornitori terzi

2.1.3. tirocinanti o personale part-time coinvolto nell'erogazione dei servizi ai clienti o con accesso ai sistemi

2.2. La politica si applica a tutte le forme di comunicazione esterna che fanno riferimento all'organizzazione, incluse:

2.2.1. pubblicazioni sui social media (LinkedIn, Twitter/X, TikTok, Instagram, Facebook, ecc.)

2.2.2. articoli di blog, forum online, recensioni dei clienti e discussioni online

2.2.3. interventi pubblici (ad es. conferenze, webinar, podcast)

2.2.4. e-mail o messaggi a giornalisti, rappresentanti istituzionali o influencer

2.2.5. screenshot, fotografie o video condivisi pubblicamente provenienti da ambienti di lavoro

2.3. La politica si applica anche quando tali comunicazioni sono effettuate:

2.3.1. da dispositivi personali o account personali

2.3.2. al di fuori del normale orario di lavoro

2.3.3. senza intento doloso: rientrano nell'ambito di applicazione anche osservazioni accidentali o estemporanee che facciano riferimento all'azienda

3. Obiettivi

3.1. Protezione della reputazione: prevenire danni all'immagine dell'azienda causati da comunicazioni pubbliche non autorizzate o inappropriate

3.2. Sicurezza dei dati: evitare l'esposizione non intenzionale di dati sensibili, sistemi interni o dettagli dei clienti tramite social media o canali pubblici

3.3. Conformità legale e regolamentare: assicurare che tutti i contenuti pubblici che fanno riferimento all'azienda siano conformi alla normativa applicabile in materia di protezione dei dati e comunicazioni commerciali

3.4. Condotta professionale: promuovere una partecipazione responsabile alle discussioni online e ai rapporti con i media, anche attraverso account personali

3.5. Preparazione agli incidenti: fornire indicazioni chiare e attuabili in caso di divulgazioni accidentali o violazioni della politica

4. Ruoli e responsabilità

4.1. Direttore generale (GM)

4.1.1. è il titolare della politica e la approva

4.1.2. riesamina e autorizza qualsiasi dichiarazione pubblica, rapporto con la stampa o intervista ai media

4.1.3. assicura che la presente politica sia comunicata in modo chiaro a tutti i dipendenti e alle terze parti

4.1.4. indaga e gestisce eventuali violazioni della presente politica, in coordinamento con le procedure di risposta agli incidenti

4.2. Dipendente designato o responsabile delle comunicazioni (se nominato)

4.2.1. supporta il GM riesaminando i contenuti prima della pubblicazione esterna (ad es. articoli di blog, temi di intervento)

4.2.2. mantiene le registrazioni delle attività mediatiche approvate o dei contenuti social ad alto rischio approvati

4.2.3. monitora, nei limiti delle capacità disponibili, le menzioni note dell'azienda online per individuare rischi reputazionali o di sicurezza

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

9. Requisiti di riesame e aggiornamento

9.1. Riesame annuale

9.1.1. La presente politica deve essere riesaminata almeno una volta all'anno dal Direttore generale (GM)

9.1.2. Il riesame deve assicurare l'allineamento con gli obblighi legali aggiornati, le tendenze del settore in materia di comunicazione e i cambiamenti organizzativi interni

9.2. Riesami attivati da eventi scatenanti

9.2.1. La presente politica deve essere aggiornata immediatamente a seguito di:

9.2.1.1. un incidente significativo sui social media o una problematica reputazionale rilevante

9.2.1.2. una modifica dei fornitori terzi che gestiscono le comunicazioni

9.2.1.3. nuova legislazione o nuovi obblighi regolamentari relativi alle comunicazioni online, ai media o all'uso del marchio

9.3. Documentazione delle modifiche

9.3.1. Tutti gli aggiornamenti devono essere registrati, inclusi la data del riesame, la sintesi delle modifiche e l'approvazione del GM

9.3.2. Deve essere mantenuta una cronologia delle versioni ai fini di audit e certificazione

9.4. Distribuzione degli aggiornamenti

9.4.1. Tutto il personale e i collaboratori esterni devono essere informati di eventuali modifiche alla politica

9.4.2. Le versioni aggiornate devono essere condivise tramite e-mail o portali interni

9.4.3. Qualsiasi fornitore che gestisca comunicazioni pubbliche deve prendere atto delle condizioni aggiornate prima di proseguire le attività

10. Politiche correlate e collegamenti

10.1. La presente politica opera in coordinamento con le seguenti politiche SME:

10.1.1. P3S – Politica di uso accettabile: definisce il comportamento consentito nell'uso delle piattaforme di comunicazione, incluso l'accesso ai social media durante l'orario di lavoro

10.1.2. P8S – Politica di consapevolezza e formazione sulla sicurezza delle informazioni: assicura che il personale sia formato a riconoscere i rischi di eccessiva condivisione, phishing o minacce reputazionali online

10.1.3. P17S – Politica di protezione dei dati e privacy: assicura che i dati personali e i dati dei clienti non siano condivisi nelle comunicazioni esterne, in allineamento con il GDPR e altri requisiti legali

10.1.4. P30S – Politica di risposta agli incidenti: disciplina la risposta alla divulgazione pubblica accidentale, alle minacce online o agli attacchi reputazionali derivanti da uso improprio dei social media

10.1.5. P37S – Politica di conformità legale e regolamentare: stabilisce i più ampi obblighi legali e contrattuali dell'organizzazione nella condivisione pubblica di contenuti

10.2. Tali politiche devono essere applicate congiuntamente per mantenere una presenza esterna sicura, rispettosa e conforme alla normativa vigente.

11. Standard e quadri di riferimento

11.1. ISO/IEC 27001

11.1.1. Clausola 5.1 – Leadership e impegno: richiede la supervisione da parte della direzione dei rischi reputazionali e dei rischi informativi

11.1.2. Clausola 6.1 – Gestione del rischio: include le esposizioni al rischio connesse alle comunicazioni

11.1.3. Clausola 8.1 – Controllo operativo: copre le regole relative alle modalità con cui le informazioni vengono comunicate all'esterno

11.2. ISO/IEC 27002

11.2.1. Controllo 5.10 – Uso accettabile delle informazioni e degli asset

11.2.2. Controllo 5.11 – Sicurezza delle informazioni nelle comunicazioni

11.3. NIST SP 800-53 Rev. 5

11.3.1. PL-4 – Regole di comportamento: disciplina la condotta appropriata nell'uso delle risorse informative

11.3.2. AU-7 – Riduzione dell'audit e generazione di report: supporta il monitoraggio dell'uso dei sistemi pubblici

11.3.3. IR-6 – Segnalazione degli incidenti: impone la risposta a violazioni reputazionali e delle comunicazioni

11.3.4. AC-22 – Contenuti accessibili pubblicamente: assicura il controllo sulle pubblicazioni esterne e sugli accessi

11.4. GDPR UE (2016/679)

11.4.1. Articolo 5 – Principi applicabili al trattamento dei dati personali (accuratezza, integrità, responsabilizzazione)

11.4.2. Articolo 32 – Sicurezza del trattamento: richiede misure di sicurezza per la condivisione pubblica

11.4.3. Articolo 33 – Notifica della violazione: si applica se dati personali vengono esposti tramite comunicazioni esterne

11.5. Direttiva NIS2 UE (2022/2555)

11.5.1. Articolo 21(2)(e) – Politiche sull'uso dei sistemi informativi, comprese le piattaforme di comunicazione

11.5.2. Articolo 21(2)(f) – Politiche per la gestione dei rischi di cibersicurezza nella catena di fornitura e sulle piattaforme pubbliche

11.6. DORA UE (2022/2554)

11.6.1. Articolo 14(4) – Obblighi di comunicazione verso clienti, terze parti e autorità a seguito di incidenti operativi

11.7. COBIT 2019

11.7.1. APO09 – Gestire gli accordi di servizio: copre la supervisione dei fornitori e delle terze parti connesse alle comunicazioni

11.7.2. DSS05 – Gestire i servizi di sicurezza: include la protezione degli asset digitali esposti al pubblico

11.7.3. EDM03 – Garantire l'ottimizzazione del rischio: pone l'accento sulla gestione dei rischi reputazionali e di conformità connessi alle comunicazioni