					Insira aqui a designação da entidade jurídica registada							
Número do documento: P36S					Título do documento: **Política de Redes Sociais e Comunicações Externas**							
Versão: 1.0		Data de entrada em vigor: 01.01.2025			Proprietário do documento:							
X	Política		Norma		Procedimento		Formulário		Registo		Outro	

Histórico de revisões				
Número da revisão	**Data da revisão**	**Alterações**	**Revisto por**	**Proprietário do processo**

Aprovações			
Nome	**Cargo**	**Data**	**Assinatura**

Alinhada com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusulas 5.1, 5.2, 6.1, 8	Liderança, gestão do risco e controlo operacional das comunicações externas
ISO/IEC 27002:2022	Controlos 5.10, 5.11	Utilização aceitável e segurança da informação nas comunicações
NIST SP 800-53 Rev.5	PL-4, AU-7, IR-6, AC-22	Regras de comportamento, auditoria, notificação de incidentes e gestão de conteúdos e acessos públicos
RGPD da UE	Artigos 5, 32, 33	Princípios de proteção de dados, segurança e notificação de violação de dados com impacto na comunicação pública
Diretiva NIS2 da UE	Artigo 21(2)(e), 21(2)(f)	Políticas para a utilização de sistemas e gestão do risco da cadeia de fornecimento/comunicações públicas
DORA da UE	Artigo 14(4)	Obrigações de comunicação na sequência de incidentes

1. Finalidade

1.1. A presente política estabelece diretrizes obrigatórias para todas as comunicações dirigidas ao público — incluindo a utilização de redes sociais, a interação com a imprensa e os conteúdos digitais externos — sempre que exista referência à empresa, ao seu pessoal, clientes, sistemas ou práticas internas.

1.2. A política visa proteger a reputação da empresa, assegurar o cumprimento legal e regulamentar e reduzir o risco de fuga de dados, desinformação ou incidentes de segurança.

1.3. A política permite que trabalhadores e parceiros participem de forma positiva e responsável em discussões online, evitando divulgações acidentais ou deturpações.

1.4. A política reforça a preparação da SME para a certificação ISO/IEC 27001, ao abranger o controlo da informação disponibilizada ao público ou a partes interessadas externas.

2. Âmbito

2.1. Esta política aplica-se a todas as pessoas com vínculo à organização, incluindo:

2.1.1. trabalhadores e prestadores de serviços

2.1.2. freelancers, consultores e fornecedores terceiros

2.1.3. estagiários ou trabalhadores a tempo parcial envolvidos na prestação de serviços ao cliente ou com acesso a sistemas

2.2. A política aplica-se a todas as formas de comunicação externa que façam referência à organização, incluindo:

2.2.1. publicações em redes sociais (LinkedIn, Twitter/X, TikTok, Instagram, Facebook, etc.)

2.2.2. artigos de blogue, fóruns online, avaliações de clientes e tópicos de discussão

2.2.3. intervenções públicas (por exemplo, conferências, webinars em direto, podcasts)

2.2.4. mensagens de correio eletrónico ou outras mensagens dirigidas a jornalistas, representantes governamentais ou influenciadores

2.2.5. capturas de ecrã, fotografias ou vídeos partilhados publicamente a partir de ambientes de trabalho

2.3. A política também se aplica quando essa comunicação é efetuada:

2.3.1. a partir de dispositivos ou contas pessoais

2.3.2. fora do horário normal de trabalho

2.3.3. sem intenção maliciosa — mesmo observações acidentais ou informais estão abrangidas se fizerem referência à empresa

3. Objetivos

3.1. Proteção da reputação: prevenir danos na imagem da empresa decorrentes de comunicação pública não autorizada ou inadequada

3.2. Segurança da informação: evitar a exposição não intencional de dados sensíveis, sistemas internos ou detalhes de clientes através de redes sociais ou canais públicos

3.3. Cumprimento legal e regulamentar: assegurar que todo o conteúdo público que faça referência à empresa cumpre a legislação aplicável em matéria de proteção de dados e comunicação empresarial

3.4. Conduta profissional: promover uma participação responsável em discussões online e interações com os meios de comunicação social, mesmo em contas pessoais

3.5. Preparação para incidentes: definir passos claros e executáveis em caso de divulgações acidentais ou violações da política

4. Papéis e responsabilidades

4.1. Diretor-Geral (DG)

4.1.1. É o responsável por esta política e aprova-a

4.1.2. Revê e autoriza quaisquer declarações públicas, interações com a imprensa ou entrevistas aos meios de comunicação social

4.1.3. Assegura que esta política é comunicada de forma clara a todos os trabalhadores e terceiros

4.1.4. Investiga e responde a quaisquer violações desta política, em articulação com os procedimentos de resposta a incidentes

4.2. Trabalhador designado ou responsável pela comunicação (quando aplicável)

4.2.1. Apoia o DG na revisão de conteúdos antes da respetiva publicação externa (por exemplo, artigos de blogue, temas de apresentações)

4.2.2. Mantém registos de atividades mediáticas aprovadas ou de publicações em redes sociais de alto risco

4.2.3. Monitoriza referências conhecidas à empresa em canais online quanto a riscos reputacionais ou de segurança, na medida da capacidade disponível

[... As secções 4.3–8 não estão incluídas nesta pré-visualização. Adquira o documento completo para aceder ao conteúdo integral. ...]

9. Requisitos de revisão e atualização

9.1. Revisão anual

9.1.1. Esta política deve ser revista pelo menos uma vez por ano pelo Diretor-Geral (DG)

9.1.2. A revisão deve assegurar o alinhamento com obrigações legais atualizadas, tendências de comunicação do setor e alterações internas do negócio

9.2. Revisões desencadeadas por eventos

9.2.1. Esta política deve ser atualizada imediatamente após:

9.2.1.1. um incidente relevante em redes sociais ou uma questão reputacional

9.2.1.2. uma alteração de fornecedores terceiros que gerem comunicações

9.2.1.3. nova legislação ou novas obrigações regulamentares relacionadas com comunicação online, meios de comunicação social ou imagem de marca

9.3. Documentação das alterações

9.3.1. Todas as atualizações devem ser registadas, incluindo a data de revisão, o resumo das alterações e a aprovação pelo DG

9.3.2. Deve ser mantido um histórico de versões para efeitos de auditoria e certificação

9.4. Distribuição das atualizações

9.4.1. Todo o pessoal e prestadores de serviços devem ser informados de quaisquer alterações às políticas

9.4.2. As versões atualizadas devem ser partilhadas por correio eletrónico ou através de portais internos

9.4.3. Qualquer fornecedor de comunicações públicas deve confirmar os termos atualizados antes de prosseguir o trabalho

10. Políticas relacionadas e ligações

10.1. Esta política funciona em articulação com as seguintes políticas SME:

10.1.1. P3S – Política de Utilização Aceitável: define o comportamento aceitável na utilização de plataformas de comunicação, incluindo o acesso a redes sociais durante o horário de trabalho

10.1.2. P8S – Política de Sensibilização e Formação em Segurança da Informação: assegura que o pessoal recebe formação para identificar os riscos de partilha excessiva, phishing ou ameaças reputacionais online

10.1.3. P17S – Política de Proteção de Dados e Privacidade: assegura que dados pessoais e dados de clientes não são partilhados em comunicações externas, em alinhamento com o RGPD da UE e outros requisitos legais

10.1.4. P30S – Política de Resposta a Incidentes: rege a resposta a divulgação pública acidental, ameaças online ou ataques reputacionais resultantes do uso indevido de redes sociais

10.1.5. P37S – Política de Cumprimento Legal e Regulamentar: estabelece as obrigações legais e contratuais mais amplas da organização quando partilha conteúdos publicamente

10.2. Estas políticas devem ser aplicadas em conjunto para manter uma presença externa segura, respeitosa e em conformidade com a lei.

11. Normas e referenciais

11.1. ISO/IEC 27001

11.1.1. Cláusula 5.1 – Liderança e compromisso: exige supervisão da liderança sobre riscos reputacionais e riscos de informação

11.1.2. Cláusula 6.1 – Gestão do risco: inclui exposições ao risco relacionadas com a comunicação

11.1.3. Cláusula 8.1 – Controlo operacional: abrange regras sobre a forma como a informação é comunicada externamente

11.2. ISO/IEC 27002

11.2.1. Controlo 5.10 – Utilização aceitável da informação e dos ativos

11.2.2. Controlo 5.11 – Segurança da informação nas comunicações

11.3. NIST SP 800-53 Rev. 5

11.3.1. PL-4 – Regras de comportamento: rege a conduta adequada na utilização de recursos de informação

11.3.2. AU-7 – Redução de auditoria e geração de relatórios: suporta a monitorização da utilização de sistemas públicos

11.3.3. IR-6 – Notificação de incidentes: impõe a resposta a violações reputacionais e de comunicação

11.3.4. AC-22 – Conteúdo publicamente acessível: assegura o controlo sobre publicações externas e acessos

11.4. RGPD da UE (2016/679)

11.4.1. Artigo 5 – Princípios relativos ao tratamento de dados pessoais (exatidão, integridade, responsabilização)

11.4.2. Artigo 32 – Segurança do tratamento: exige salvaguardas em torno da partilha pública

11.4.3. Artigo 33 – Notificação de violação de dados: é acionado se dados pessoais forem expostos por comunicação externa

11.5. Diretiva NIS2 da UE (2022/2555)

11.5.1. Artigo 21(2)(e) – Políticas sobre a utilização de sistemas de informação, incluindo plataformas de comunicação

11.5.2. Artigo 21(2)(f) – Políticas para tratar riscos de cibersegurança na cadeia de fornecimento e em plataformas públicas

11.6. DORA da UE (2022/2554)

11.6.1. Artigo 14(4) – Obrigações de comunicação a clientes, terceiros e autoridades na sequência de incidentes operacionais

11.7. COBIT 2019

11.7.1. APO09 – Gerir acordos de nível de serviço: abrange a supervisão de fornecedores e de terceiros relacionados com comunicações

11.7.2. DSS05 – Gerir serviços de segurança: inclui a proteção de ativos digitais expostos ao público

11.7.3. EDM03 – Assegurar a otimização do risco: enfatiza a gestão de riscos reputacionais e de conformidade relacionados com a comunicação