					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P36S					Titre du document : **Politique relative aux médias sociaux et aux communications externes**							
Version : 1.0		Date d'entrée en vigueur : 01.01.2025			Propriétaire du document :							
X	Politique		Norme		Procédure		Formulaire		Registre		Autre	

Historique des révisions				
Numéro de révision	**Date de révision**	**Modifications**	**Revu par**	**Propriétaire du processus**

Approbations			
Nom	**Fonction**	**Date**	**Signature**

Alignement sur les normes et réglementations

Norme/Réglementation	Clause/Article	Commentaire
ISO/IEC 27001:2022	Articles 5.1, 5.2, 6.1, 8	Leadership, gestion des risques et contrôle opérationnel des communications externes
ISO/IEC 27002:2022	Mesures 5.10, 5.11	Utilisation acceptable et sécurité de l'information dans les communications
NIST SP 800-53 Rev. 5	PL-4, AU-7, IR-6, AC-22	Règles de comportement, audit, signalement des incidents et gestion des contenus et accès publics
RGPD de l'UE	Articles 5, 32, 33	Principes de protection des données, sécurité et notification des violations de données affectant la communication publique
NIS2 de l'UE	Article 21(2)(e), 21(2)(f)	Politiques d'utilisation des systèmes et gestion des risques liés aux communications publiques et à la chaîne d'approvisionnement
DORA de l'UE	Article 14(4)	Obligations de communication après incident

1. Objet

1.1. La présente politique définit des règles obligatoires applicables à toute communication à destination du public — y compris l'utilisation des médias sociaux, les échanges avec la presse et les contenus numériques externes — dès lors qu'elle fait référence à l'entreprise, à son personnel, à ses clients, à ses systèmes ou à ses pratiques internes.

1.2. Cette politique a pour objet de protéger la réputation de l'entreprise, de maintenir la conformité légale et réglementaire et de réduire le risque de fuite d'informations, de désinformation ou d'incident de sécurité.

1.3. Elle permet au personnel et aux partenaires de participer de manière positive et responsable aux échanges en ligne, tout en évitant les divulgations accidentelles ou les présentations inexactes.

1.4. Elle renforce l'état de préparation de la PME à la certification ISO/IEC 27001 en encadrant le contrôle des informations mises à la disposition du public ou des parties prenantes externes.

2. Champ d’application

2.1. La présente politique s'applique à toute personne liée à l'organisation, notamment :

2.1.1. les employés et les prestataires

2.1.2. les travailleurs indépendants, les consultants et les fournisseurs tiers

2.1.3. les stagiaires ou collaborateurs à temps partiel impliqués dans la fourniture de services aux clients ou disposant d'un accès aux systèmes

2.2. La présente politique s'applique à toute forme de communication externe faisant référence à l'organisation, notamment :

2.2.1. les publications sur les médias sociaux (LinkedIn, Twitter/X, TikTok, Instagram, Facebook, etc.)

2.2.2. les billets de blog, forums en ligne, avis clients et fils de discussion

2.2.3. les interventions publiques (par exemple : conférences, webinaires, podcasts)

2.2.4. les courriels ou messages adressés à des journalistes, représentants des pouvoirs publics ou influenceurs

2.2.5. les captures d'écran, photos ou vidéos partagées publiquement depuis des environnements de travail

2.3. La présente politique s'applique également lorsque cette communication est effectuée :

2.3.1. depuis des appareils ou comptes personnels

2.3.2. en dehors des heures normales de travail

2.3.3. sans intention malveillante — y compris lorsque les propos sont accidentels ou informels dès lors qu'ils font référence à l'entreprise

3. Objectifs

3.1. Protection de la réputation : prévenir toute atteinte à l'image de l'entreprise résultant d'une communication publique non autorisée ou inappropriée

3.2. Sécurité des données : éviter l'exposition non intentionnelle de données sensibles, de systèmes internes ou d'informations clients via les médias sociaux ou d'autres canaux publics

3.3. Conformité légale et réglementaire : garantir que tout contenu public faisant référence à l'entreprise respecte les lois applicables en matière de protection des données et de communication commerciale

3.4. Comportement professionnel : promouvoir une participation responsable aux échanges en ligne et aux interactions avec les médias, y compris via des comptes personnels

3.5. Préparation aux incidents : définir des mesures claires et applicables en cas de divulgation accidentelle ou de manquement à la politique

4. Rôles et responsabilités

4.1. Directeur général (DG)

4.1.1. est responsable de la présente politique et l'approuve

4.1.2. examine et autorise toute déclaration publique, interaction avec la presse ou interview dans les médias

4.1.3. veille à ce que cette politique soit clairement communiquée à l'ensemble des employés et des tiers

4.1.4. enquête sur tout manquement à la présente politique et y répond, en coordination avec les procédures de réponse aux incidents

4.2. Employé désigné ou responsable de la communication (le cas échéant)

4.2.1. assiste le DG en examinant les contenus avant toute publication externe (par exemple : billets de blog, sujets d'intervention)

4.2.2. tient un registre des activités médiatiques approuvées ou des publications sur les médias sociaux à haut risque

4.2.3. surveille, dans la mesure des capacités disponibles, les mentions connues de l'entreprise en ligne afin d'identifier les risques réputationnels ou de sécurité

[... Les sections 4.3–8 ne sont pas incluses dans cet aperçu. Achetez le document complet pour accéder à l'intégralité du contenu. ...]

9. Exigences de revue et de mise à jour

9.1. Revue annuelle

9.1.1. La présente politique doit être revue au moins une fois par an par le directeur général (DG)

9.1.2. Cette revue doit garantir l'alignement avec les obligations légales mises à jour, l'évolution des pratiques de communication du secteur et les changements internes de l'activité

9.2. Revues déclenchées par événement

9.2.1. La présente politique doit être mise à jour immédiatement après :

9.2.1.1. un incident significatif lié aux médias sociaux ou un enjeu réputationnel majeur

9.2.1.2. un changement de fournisseurs tiers chargés de gérer les communications

9.2.1.3. une nouvelle législation ou de nouvelles obligations réglementaires relatives à la communication en ligne, aux médias ou à l'image de marque

9.3. Documentation des modifications

9.3.1. Toute mise à jour doit être consignée, y compris la date de revue, le résumé des modifications et l'approbation du DG

9.3.2. Un historique des versions doit être conservé à des fins d'audit et de certification

9.4. Diffusion des mises à jour

9.4.1. L'ensemble du personnel et les prestataires doivent être informés de toute modification de la politique

9.4.2. Les versions mises à jour doivent être diffusées par courriel ou via des portails internes

9.4.3. Tout fournisseur de services de communication publique doit accuser réception des dispositions mises à jour avant de poursuivre ses activités

10. Politiques associées et articulations

10.1. La présente politique s'applique en articulation avec les politiques PME suivantes :

10.1.1. P3S – Politique d'utilisation acceptable : définit les comportements autorisés lors de l'utilisation des plateformes de communication, y compris l'accès aux médias sociaux pendant les heures de travail

10.1.2. P8S – Politique de sensibilisation et de formation à la sécurité de l'information : garantit que le personnel est formé à identifier les risques de surpartage d'informations, de phishing ou de menaces réputationnelles en ligne

10.1.3. P17S – Politique de protection des données et de la vie privée : garantit que les données à caractère personnel et les données clients ne sont pas partagées dans les communications externes, en conformité avec le RGPD et les autres exigences légales

10.1.4. P30S – Politique de réponse aux incidents : encadre la réponse aux divulgations publiques accidentelles, aux menaces en ligne ou aux atteintes réputationnelles résultant d'un usage inapproprié des médias sociaux

10.1.5. P37S – Politique de conformité légale et réglementaire : définit les obligations légales et contractuelles plus larges de l'organisation lorsqu'elle partage publiquement des contenus

10.2. Ces politiques doivent être appliquées conjointement afin de maintenir une présence externe sûre, respectueuse et conforme aux exigences légales.

11. Normes et référentiels de référence

11.1. ISO/IEC 27001

11.1.1. Article 5.1 – Leadership et engagement : exige une supervision par la direction des risques réputationnels et des risques liés à l'information

11.1.2. Article 6.1 – Gestion des risques : inclut les expositions aux risques liées aux communications

11.1.3. Article 8.1 – Contrôle opérationnel : couvre les règles encadrant la communication externe des informations

11.2. ISO/IEC 27002

11.2.1. Mesure 5.10 – Utilisation acceptable des informations et des actifs

11.2.2. Mesure 5.11 – Sécurité de l'information dans les communications

11.3. NIST SP 800-53 Rev. 5

11.3.1. PL-4 – Règles de comportement : encadre le comportement approprié lors de l'utilisation des ressources d'information

11.3.2. AU-7 – Réduction des données d'audit et génération de rapports : soutient la surveillance de l'utilisation publique des systèmes

11.3.3. IR-6 – Signalement des incidents : impose une réponse aux atteintes réputationnelles et aux violations liées aux communications

11.3.4. AC-22 – Contenu accessible au public : garantit le contrôle des publications externes et des accès associés

11.4. RGPD de l'UE (2016/679)

11.4.1. Article 5 – Principes relatifs au traitement des données à caractère personnel (exactitude, intégrité, responsabilité)

11.4.2. Article 32 – Sécurité du traitement : exige des mesures de protection encadrant le partage public

11.4.3. Article 33 – Notification de violation : s'applique si des données à caractère personnel sont exposées via une communication externe

11.5. Directive NIS2 de l'UE (2022/2555)

11.5.1. Article 21(2)(e) – Politiques d'utilisation des systèmes d'information, y compris des plateformes de communication

11.5.2. Article 21(2)(f) – Politiques de gestion des risques de cybersécurité dans la chaîne d'approvisionnement et sur les plateformes publiques

11.6. DORA de l'UE (2022/2554)

11.6.1. Article 14(4) – Obligations de communication envers les clients, les tiers et les autorités à la suite d'incidents opérationnels

11.7. COBIT 2019

11.7.1. APO09 – Gérer les accords de service : couvre la supervision des fournisseurs et des tiers liés aux communications

11.7.2. DSS05 – Gérer les services de sécurité : inclut la protection des actifs numériques exposés au public

11.7.3. EDM03 – Garantir l'optimisation des risques : met l'accent sur la gestion des risques réputationnels et de conformité liés à la communication