					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P36					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 lorsque applicable

Alignement sur les normes et réglementations

Norme/Réglementation	Clause/Article	Commentaire
ISO/IEC 27001:2022	Clause 8	Processus définis et gouvernance fondée sur les rôles pour la gestion des communications publiques, garantissant l'exactitude, les circuits d'approbation et l'escalade des incidents.
ISO/IEC 27002:2022	Contrôles 5.10, 5.11, 5.35, 5.36	Encadre l'utilisation de l'information, l'utilisation acceptable, les communications externes avec les autorités et l'établissement de rapports de conformité.
NIST SP 800-53 Rév. 5	AC-8, AU-12, PL-4	Règles relatives à l'utilisation des systèmes et des communications, aux notifications aux utilisateurs et à la conservation des journaux d'audit.
RGPD de l'UE	Articles 5, 25, 32, 33	Principes de traitement des données, protection des données dès la conception, sécurité du traitement et obligations de notification des violations de données.
NIS2 de l'UE	Article 21	Mesures de gestion des risques de cybersécurité, obligations en cas d'incident et encadrement des communications publiques liées au risque.
DORA de l'UE	Articles 9, 16	Gestion des risques liés aux TIC et stratégie de communication pour les prestataires critiques.
COBIT 2019	APO09, DSS05	Gouvernance des accords de service et des communications, ainsi que pratiques de communication sécurisée et de gestion des incidents.

1. Objet

1.1 La présente politique établit des règles et responsabilités obligatoires encadrant l'usage des médias sociaux et toutes les formes de communication externe par le personnel affilié à l'organisation.

1.2 Elle vise à garantir que tout message public — planifié ou spontané — soit exact, respectueux, sécurisé, conforme aux exigences légales et cohérent avec l'image de marque.

1.3 La politique a pour objectif de réduire les risques liés aux atteintes à la réputation, aux manquements réglementaires, aux fuites de propriété intellectuelle et aux divulgations non autorisées via des canaux exposés au public.

1.4 Elle promeut en outre la responsabilisation et une gouvernance structurée dans toutes les formes de communication numérique impliquant l'organisation ou ayant une incidence sur celle-ci.

2. Champ d'application

2.1 La présente politique s'applique à tous les employés, prestataires, stagiaires et représentants tiers qui :

2.1.1 communiquent au nom de l'organisation, à titre officiel ou informel ;

2.1.2 font référence à l'organisation ou laissent entendre un lien d'affiliation avec celle-ci dans un contexte public ;

2.1.3 utilisent des comptes personnels ou d'entreprise pour participer à des discussions publiques impliquant l'organisation.

2.2 Les canaux de communication couverts comprennent notamment :

2.2.1 les plateformes de médias sociaux (par exemple : LinkedIn, X/Twitter, Instagram, TikTok, YouTube, Facebook) ;

2.2.2 les blogs, wikis, forums et espaces de discussion publics ;

2.2.3 le courrier électronique ou la messagerie directe à destination de parties externes (par exemple : clients, autorités de régulation, médias) ;

2.2.4 les interviews de presse, tables rondes, interventions publiques ou apparitions dans des médias enregistrés ;

2.2.5 la participation à des communautés en ligne dans lesquelles l'organisation est mentionnée.

2.3 La présente politique encadre à la fois les contenus diffusés en temps réel et les contenus programmés à l'avance, et s'applique à tous les appareils et comptes (personnels ou d'entreprise) utilisés pour diffuser la communication.

3. Objectifs

3.1 Prévenir la divulgation accidentelle ou intentionnelle d'informations confidentielles, sensibles ou réglementées via des canaux de communication externe.

3.2 Garantir que les déclarations publiques officielles et les contenus publiés sur les médias sociaux soient exacts, autorisés et alignés sur l'image de marque, l'éthique et les messages stratégiques de l'entreprise.

3.3 Prévenir les atteintes à la réputation et imposer la cohérence des messages entre les départements internes et les plateformes externes.

3.4 Respecter les obligations légales applicables relatives aux déclarations publiques, y compris, sans s'y limiter, celles découlant du RGPD, de NIS2, de DORA et des règles sectorielles en matière de communication.

3.5 Définir des responsabilités claires, des cas d'usage autorisés et des modalités d'application pour l'ensemble du personnel impliqué dans des activités exposées au public.

4. Rôles et responsabilités

4.1 Directeur marketing ou communication / Responsable des relations publiques

4.1.1 Approuve tous les messages officiels de l'entreprise destinés à une publication externe.

4.1.2 Tient à jour les calendriers éditoriaux des médias sociaux et les lignes directrices garantissant la cohérence de l'image de marque.

4.1.3 Assure la surveillance des mentions en ligne et de l’exposition médiatique concernant l’organisation.

4.2 Responsable de la sécurité des systèmes d’information (RSSI) / Équipe de sécurité de l’information

4.2.1 Assure la surveillance des plateformes numériques afin de détecter les indicateurs de fuite de données, d’usurpation d’identité ou de tentatives d’hameçonnage.

4.2.2 Se coordonne avec les équipes de réponse aux incidents en cas d’attaques ou de violations liées aux médias sociaux.

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

9.1 La présente politique est obligatoire pour l’ensemble du personnel concerné et des tiers. Tout non-respect peut entraîner :

9.1.1 des avertissements formels ;

9.1.2 une révocation temporaire ou permanente des accès aux plateformes ou aux systèmes ;

9.1.3 des sanctions disciplinaires, y compris la cessation de la relation de travail ou contractuelle ;

9.1.4 des poursuites judiciaires, si la communication externe entraîne un préjudice réputationnel, une violation de données ou une non-conformité réglementaire.

9.2 Sanctions disciplinaires

9.2.1 Les manquements internes (par exemple : fuite de données confidentielles, diffamation de l’organisation) entraînent l’intervention des ressources humaines, une enquête formelle et une documentation dans le dossier du salarié.

9.2.2 Le cas échéant, le service juridique engage des recours civils ou notifie les autorités en cas d’activité pénale (par exemple : usurpation d’identité, fuite d’informations liées à un délit d’initié).

9.3 Surveillance de la conformité

9.3.1 Les équipes Sécurité et Communication doivent assurer une surveillance continue de :

9.3.1.1 les mentions de la marque sur les principales plateformes ;

9.3.1.2 l’utilisation non officielle des visuels de l’entreprise ou de ses marques ;

9.3.1.3 les risques connus (par exemple : employés mécontents, tentatives d’usurpation d’identité).

9.3.2 La surveillance doit être conforme aux lois et réglementations relatives à la vie privée des salariés, et tout cas signalé doit être vérifié par un examinateur humain.

9.4 Dispositif d’alerte et signalement des usages abusifs

9.4.1 Tout employé soupçonnant un manquement à la présente politique est encouragé à le signaler à l’équipe de sécurité de l’information, au service juridique, ou de manière anonyme via le portail du dispositif d’alerte.

9.4.2 Toute mesure de rétorsion à l’encontre d’un lanceur d’alerte est strictement interdite et fait l’objet d’une action disciplinaire immédiate.

10. Exigences de revue et de mise à jour

10.1 La présente politique doit faire l’objet d’une revue annuelle, ou plus tôt si :

10.1.1 des changements significatifs interviennent dans les exigences réglementaires (par exemple : nouvelles règles de l’UE relatives aux communications numériques) ;

10.1.2 de nouvelles plateformes sociales ou de nouveaux canaux de communication sont adoptés ;

10.1.3 un incident significatif ou des manquements répétés révèlent des lacunes de processus ;

10.1.4 un changement structurel ou de direction affecte les fonctions relations publiques, juridique ou sécurité.

10.2 La revue doit être réalisée conjointement par :

10.2.1 le responsable Marketing / Relations publiques ;

10.2.2 le RSSI ou le responsable des risques de sécurité ;

10.2.3 les responsables juridique et conformité.

10.3 Les mises à jour doivent être documentées dans le registre des modifications de politique et communiquées par les canaux internes de sensibilisation. En cas de changement significatif, tout le personnel concerné doit confirmer à nouveau sa prise de connaissance de la politique.

11. Politiques associées et articulations

11.1 La présente politique est soutenue par les composantes suivantes du système de management de la sécurité de l'information (SMSI) de l'organisation et s'articule avec elles :

11.1.1 P1 – Politique de sécurité de l'information : établit les principes directeurs de protection de l'information, y compris l'exigence que les communications n'entraînent pas de divulgation non autorisée.

11.1.2 P3 – Politique d'utilisation acceptable : définit les comportements acceptables sur les plateformes et technologies numériques, qui encadrent directement l'usage personnel et professionnel des canaux sociaux.

11.1.3 P6 – Politique de gestion des risques : fournit le cadre de gestion des risques pour l'évaluation des menaces liées à la communication publique et à l'exposition réputationnelle.

11.1.4 P8 – Politique de sensibilisation et de formation à la sécurité de l'information : impose des programmes de sensibilisation destinés à former le personnel aux pratiques de communication sécurisée et aux menaces d'ingénierie sociale.

11.1.5 P13 – Politique de classification et d'étiquetage des données : guide le personnel sur ce qui constitue une information restreinte ou confidentielle et ne doit pas être divulgué à l'extérieur.

11.1.6 P30 – Politique de réponse aux incidents : définit la manière de traiter les incidents liés aux communications publiques, y compris les fuites de données, l'usurpation d'identité et les manquements réglementaires.

11.1.7 P33 – Politique d'audit et de surveillance de la conformité : encadre les processus d'audit qui valident les contrôles relatifs aux médias sociaux, les systèmes de surveillance et la conformité aux politiques de communication externe.

12. Normes et référentiels de référence

12.1 ISO/IEC 27001:

12.1.1 Clause 8.1 – Planification et maîtrise opérationnelles : exige des processus définis et une gouvernance fondée sur les rôles pour la gestion des communications publiques, garantissant l'exactitude, les circuits d'approbation et l'escalade des incidents impliquant un risque pour les données ou la réputation.

12.2 ISO/IEC 27002:2022:

12.2.1 Contrôle 5.10 – Utilisation de l'information : encadre la diffusion autorisée et éthique des communications internes ou externes.

12.2.2 Contrôle 5.11 – Utilisation acceptable de l'information et des actifs : renforce les pratiques acceptables de partage de contenu au moyen des actifs de l'entreprise ou de comptes personnels.

12.2.3 Contrôle 5.35 – Contact avec les autorités : exige une communication externe structurée et autorisée avec les autorités de régulation et les organismes publics.

12.2.4 Contrôle 5.36 – Conformité aux politiques et normes : impose l'application cohérente des politiques internes dans tous les scénarios de communication.

12.3 NIST SP 800-53 Rév. 5:

12.3.1 PL-4 – Règles de comportement : exige des règles formelles d'utilisation des systèmes et des communications, y compris des normes relatives à la divulgation publique.

12.3.2 AC-8 – Notification d'utilisation du système : prend en charge les avertissements obligatoires et les messages d'alerte sur les plateformes exposées à l'extérieur.

12.3.3 AU-12 – Conservation des enregistrements d'audit : s'applique à la conservation des journaux et de l'historique des communications à des fins de revue d'incident et d'audit.

12.4 RGPD de l'UE (2016/679):

12.4.1 Article 5 – Principes du traitement des données : interdit le partage non autorisé de données à caractère personnel par des communications publiques.

12.4.2 Article 25 – Protection des données dès la conception et par défaut : exige des mesures de protection de la vie privée dans les outils de communication et les circuits de contenu.

12.4.3 Article 32 – Sécurité du traitement : couvre le chiffrement, le contrôle d'accès et les processus d'approbation des contenus.

12.4.4 Article 33 – Notification de violation : impose une notification en temps utile des fuites de données à caractère personnel via des canaux publics.

12.5 Directive NIS2 de l'UE (2022/2555):

12.5.1 Article 21 – Mesures de gestion des risques de cybersécurité : inclut les protocoles de communication, les obligations en cas d'incident ainsi que les messages publics relatifs au risque.

12.6 DORA de l'UE (2022/2554):

12.6.1 Article 9 – Gestion des risques liés aux TIC : s'applique aux risques de communication d'origine externe, tels que l'usurpation d'identité, la désinformation et les atteintes à la réputation.

12.6.2 Article 16 – Stratégie de communication : exige que les prestataires critiques de services financiers gèrent les risques de communication et les réponses associées en situation de crise.

12.7 COBIT 2019:

12.7.1 APO09 – Gestion des accords de service et de la communication : exige une gouvernance structurée des communications internes et externes.

12.7.2 DSS05 – Gestion des services de sécurité : garantit que les activités de communication n'introduisent pas de risque supplémentaire et ne compromettent pas les processus de gestion des incidents.