					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P03					Titre du document : **Politique d'utilisation acceptable**							
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	Clause 5	Définit les règles de comportement et les exigences applicables à la politique d'utilisation acceptable
ISO/IEC 27002:2022	Contrôles 6.1, 6.2, 8.1, 8.12	Précise les responsabilités en matière de sécurité de l'information, la sensibilisation, ainsi que la gouvernance des équipements et des données
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Contrôles d'accès et mesures de sensibilisation/comportement applicables à l'utilisation des actifs informatiques
RGPD de l'UE	Articles 5(1)(f), 32 ; considérant 39	Imposent la confidentialité et l'intégrité, exigent des mesures techniques et organisationnelles, ainsi que des bases légales pour un usage approprié
NIS2 de l'UE	Article 21(2)(a–d)	Imposent des politiques opérationnelles et une formation à l'utilisation sécurisée
DORA de l'UE	Article 5	Soutient la gestion des risques liés aux TIC en encadrant le comportement des utilisateurs
COBIT 2019	APO07, BAI05, DSS05, MEA01	Ressources humaines, conduite du changement, gestion de la sécurité, surveillance de la conformité et de la performance

1. Objet

1.1 La présente politique définit les usages autorisés et non autorisés des systèmes d'information, des ressources informatiques, des outils de communication et des pratiques de traitement des données de l'organisation.

1.2 Elle garantit que tous les utilisateurs comprennent leurs responsabilités lorsqu'ils utilisent les actifs informatiques de l'entreprise et que leurs actions contribuent à la confidentialité, à l'intégrité, à la disponibilité et au traitement licite des informations.

1.3 La présente politique satisfait à l'exigence du contrôle 5.10 de l'ISO/IEC 27001:2022 en établissant des règles de comportement relatives à l'utilisation des systèmes et en prévoyant des mesures techniques et procédurales pour réduire le risque d'usage inapproprié, de négligence ou d'abus.

1.4 Elle soutient également les activités d'investigation et d'application, y compris la réponse aux incidents et les mesures disciplinaires en cas de violation.

2. Champ d'application

2.1 La présente politique s'applique à toute personne physique ou morale disposant d'un accès aux systèmes d'information et aux actifs de l'organisation, y compris, sans s'y limiter :

2.1.1 Les salariés, prestataires, consultants, stagiaires et personnels intérimaires

2.1.2 Les fournisseurs tiers disposant d'un accès aux systèmes ou de rôles d'administration délégués

2.1.3 Les visiteurs ou partenaires utilisant une infrastructure informatique appartenant à l'organisation ou autorisée par celle-ci

2.2 Le champ d'application couvre l'ensemble des actifs technologiques et des actifs de données de l'organisation, notamment :

2.2.1 Les postes de travail, ordinateurs portables, appareils mobiles et serveurs

2.2.2 L'infrastructure réseau et les services hébergés dans le cloud

2.2.3 La messagerie électronique, la messagerie instantanée, le stockage de fichiers, les plateformes collaboratives et les VPN

2.2.4 Les données au repos, en transit ou en cours de traitement, quel qu'en soit le format ou l'emplacement

2.2.5 Tout équipement personnel utilisé dans le cadre d'un dispositif BYOD (Bring Your Own Device) et connecté aux systèmes de l'organisation

2.3 La présente politique s'applique dans tous les environnements de travail, notamment :

2.3.1 Les bureaux de l'entreprise et les sites de production

2.3.2 Les lieux de télétravail ou les dispositifs hybrides

2.3.3 Les opérations sur le terrain ou les locaux gérés par des tiers

2.4 Tous les utilisateurs doivent accuser réception de la présente politique et s'y conformer comme condition d'accès aux systèmes de l'entreprise ou de traitement des données de l'entreprise.

3. Objectifs

3.1 Définir et faire respecter des règles d'utilisation acceptable des ressources informatiques de l'organisation.

3.2 Prévenir les accès non autorisés, les fuites de données ou les dommages résultant d'un usage négligent ou malveillant.

3.3 Protéger les réseaux, les actifs et les données de l'entreprise contre les menaces introduites par le comportement des utilisateurs.

3.4 Soutenir les obligations légales et contractuelles en démontrant une diligence raisonnable dans la gouvernance des ressources informatiques.

3.5 Garantir la cohérence et la clarté dans l'application des mesures disciplinaires et des processus de gestion des exceptions.

3.6 Promouvoir une culture d'utilisation éthique, sécurisée et responsable des ressources informatiques, numériques et physiques.

4. Rôles et responsabilités

4.1 Direction générale

4.1.1 Approuve la politique d'utilisation acceptable (AUP) et veille à son alignement avec les objectifs métier, les exigences réglementaires et les valeurs de l'organisation.

4.1.2 Alloue les ressources nécessaires à l'application, à la formation, à la surveillance et à la revue de la politique.

4.1.3 Examine l'état de conformité et les mesures disciplinaires liées aux violations de la politique dans le cadre de la gouvernance du SMSI.

4.2 Équipes informatiques et de sécurité de l'information

4.2.1 Mettent en œuvre des mesures techniques pour faire appliquer la présente politique, notamment :

4.2.2 Des dispositifs de filtrage de contenu, de protection contre les logiciels malveillants, de sécurité des terminaux et des outils de surveillance du réseau

4.2.3 Des configurations de sécurité de la messagerie et des solutions de prévention des pertes de données (DLP)

4.2.4 Des listes de blocage et des listes d'autorisation pour les logiciels, matériels et sites web

4.2.5 Tiennent à jour un inventaire des logiciels, équipements et services autorisés et interdits.

4.2.6 Enquêtent sur les suspicions de violation de l'AUP, collectent les éléments de preuve forensiques et appuient, le cas échéant, les mesures disciplinaires ou les actions en justice.

4.2.7 Collaborent avec les ressources humaines et la direction juridique pour la gestion des incidents, l'escalade et les obligations de notification.

[... 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 Déclencheurs et fréquence de revue

9.1.1 La présente politique doit faire l'objet d'une revue :

9.1.1.1 Au moins une fois par an

9.1.1.2 À la suite de toute modification significative des technologies ou de l'infrastructure

9.1.1.3 Après des incidents ou des constats d'audit mettant en évidence des lacunes dans l'application de la politique

9.1.1.4 En réponse à des évolutions des lois applicables ou des obligations contractuelles

9.2 Propriété et approbation

9.2.1 Le RSSI ou le responsable désigné du SMSI est responsable du processus de revue.

9.2.2 Les mises à jour doivent être approuvées par la direction générale et communiquées à l'ensemble de l'organisation.

9.2.3 L'accusé de réception des dispositions mises à jour doit être recueilli à nouveau lors de la republication de la politique.

9.3 Gestion documentaire

9.3.1 La politique doit inclure les métadonnées et informations de gestion de version suivantes :

9.3.1.1 Le titre, l'identifiant et le niveau de classification

9.3.1.2 Le propriétaire de la politique et le responsable de la gestion documentaire

9.3.1.3 L'historique des modifications et la justification des mises à jour

9.3.1.4 Les dates de revue et de prochaine mise à jour planifiée

9.3.1.5 Les références du registre de diffusion et des accusés de réception

9.3.2 L'exemplaire maître doit être conservé dans le référentiel documentaire du SMSI sous contrôle de version.

10. Politiques associées et articulations

10.1 La présente politique doit être interprétée conjointement avec les documents suivants :

10.1.1 P1 – Politique de sécurité de l'information : établit les attentes fondamentales en matière de comportement et l'engagement de la direction en faveur de l'utilisation acceptable.

10.1.2 P4 – Politique de contrôle d'accès : définit les autorisations et droits associés aux utilisateurs, aux systèmes et à l'accès aux données, et encadre directement les limites d'utilisation acceptable.

10.1.3 P6 – Politique de gestion des risques : traite les risques liés au comportement et soutient les activités de surveillance et de traitement associées aux menaces induites par les utilisateurs.

10.1.4 P7 – Politique d'intégration et de départ : garantit la prise de connaissance des règles d'utilisation acceptable à l'entrée et la révocation des accès au départ.

10.1.5 P9 – Politique de télétravail : étend les dispositions d'utilisation acceptable aux environnements de travail à distance et hybrides.

10.2 Ces politiques associées constituent un modèle de défense en profondeur pour la gouvernance comportementale, technique et contractuelle.

11. Normes et référentiels de référence

11.1 La présente politique d'utilisation acceptable (AUP) est alignée sur des normes reconnues à l'international et des cadres juridiques afin de garantir des contrôles comportementaux opposables, auditables et fondés sur les risques pour l'ensemble des usages des systèmes d'information, qu'ils soient numériques ou physiques.

11.2 ISO/IEC 27001:2022

11.2.1 Contrôle 5.10 – Utilisation acceptable des informations et des autres actifs associés : la présente politique répond directement à l'exigence consistant à définir, communiquer et faire appliquer les règles encadrant l'usage approprié des ressources informatiques.

11.2.2 Annexe A, contrôle 6.1 – Responsabilité en matière de sécurité de l'information : attribue des responsabilités claires concernant le comportement des utilisateurs et la supervision de la conformité.

11.2.3 Annexe A, contrôle 6.2 – Sensibilisation, éducation et formation à la sécurité de l'information : les processus de formation intégrés et d'accusé de réception de la politique font partie de l'application de l'AUP.

11.2.4 Annexe A, contrôle 8.1 – Terminaux utilisateurs et contrôle 8.12 – Prévention des pertes de données : traite des comportements acceptables sur les équipements utilisateurs et encadre les activités susceptibles d'entraîner une exposition ou une fuite de données.

11.3 NIST SP 800-53 Rev.5 :

11.3.1 AC-19 (Contrôle d'accès pour les appareils mobiles) et AC-20 (Utilisation de systèmes d'information externes) : la présente politique définit les obligations et restrictions applicables aux utilisateurs en matière de BYOD et d'accès à des systèmes tiers.

11.3.2 PL-4 (Règles de comportement) : fournit des exigences détaillées d'utilisation acceptable cohérentes avec la présente politique.

11.3.3 AT-2 (Formation de sensibilisation à la sécurité) : soutenu par la formation des utilisateurs et l'accusé de réception documenté de la politique.

11.3.4 AU-2 (Événements d'audit) et AU-12 (Génération d'audit) : l'application de la politique repose sur la surveillance des actions des utilisateurs et sur l'émission d'alertes en cas de violation.

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

11.4.1 Article 5(1)(f) : impose la sécurité et l'intégrité des données à caractère personnel ; la présente politique réduit les risques introduits par le comportement humain et l'usage non autorisé.

11.4.2 Article 32 : exige des mesures techniques et organisationnelles — telles que des contrôles comportementaux et des restrictions d'usage — pour protéger les données à caractère personnel.

11.4.3 Considérant 39 : souligne la nécessité de garantir que seules les personnes autorisées disposent de l'accès nécessaire et d'un usage licite des données.

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

11.5.1 Article 21(2)(a–d) : exige des politiques opérationnelles et des formations pour une utilisation sécurisée des systèmes, que la présente AUP met en place en définissant les comportements, la surveillance et les processus d'application.

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

11.6.1 Article 5 : la présente politique soutient le cadre de gestion des risques liés aux TIC en définissant des règles d'interaction entre l'humain et les systèmes et en réduisant l'exposition aux cyberrisques liés aux comportements.

11.7 COBIT 2019 :

11.7.1 APO07 – Gestion des ressources humaines : impose les responsabilités des utilisateurs et la sensibilisation tout au long du cycle de vie du personnel.

11.7.2 BAI05 – Gestion du changement organisationnel : intègre la gouvernance de l'utilisation acceptable dans les processus de changement affectant le comportement des utilisateurs.

11.7.3 DSS05 – Gestion des services de sécurité : soutient la surveillance des activités des utilisateurs, les alertes comportementales et les mécanismes de réponse automatisés.

11.7.4 MEA01 – Surveillance, évaluation et appréciation de la performance et de la conformité : la politique définit les indicateurs et mécanismes permettant de valider la conformité des utilisateurs aux attentes comportementales.