					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P03S					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	Pertinent pour le périmètre global de la politique et sa mise en œuvre
ISO/IEC 27002:2022	5.10, 5.11, 5	Fournit des lignes directrices relatives aux exigences et mesures de contrôle en matière d'utilisation acceptable
NIST SP 800-53 Rév. 5	AC-19, AC-20, AT-2	Couvre l'utilisation des systèmes et des équipements, la surveillance et la formation des utilisateurs
RGPD de l'UE	Articles 5(1)(f), 32	Intégrité et confidentialité des données, ainsi que mesures de sécurité
NIS2 de l'UE	Article 21(2)(b)	Impose des politiques de sécurité et d'utilisation acceptable appropriées
DORA de l'UE	Article 9	Politique de gestion des risques liés aux TIC, mesures de contrôle et application
COBIT 2019	DSS05, BAI08	Services de sécurité et gestion des connaissances

1. Objet

1.1. La présente politique définit les règles d'utilisation acceptable, responsable et sécurisée des systèmes, des équipements, de l'accès à Internet, des services de messagerie, des services cloud fournis par l'entreprise, ainsi que de tout équipement personnel utilisé à des fins professionnelles.

1.2. Elle vise à garantir que les personnes concernées comprennent leurs obligations lorsqu'elles utilisent les ressources informatiques de l'organisation, afin de protéger l'intégrité des données, la vie privée et la continuité des activités.

1.3. La présente politique contribue à la conformité à l'ISO/IEC 27001:2022 en imposant des règles claires de comportement des utilisateurs, alignées sur les exigences légales, contractuelles et réglementaires.

2. Périmètre

2.1. La présente politique s'applique à toute personne qui accède aux systèmes ou aux données de l'entreprise, les administre ou interagit avec eux, y compris :

2.1.1. Les employés et les prestataires

2.1.2. Les travailleurs temporaires et les stagiaires

2.1.3. Les prestataires externes de services informatiques

2.2. Elle couvre :

2.2.1. Les ordinateurs, téléphones et tablettes appartenant à l'entreprise

2.2.2. Les équipements personnels approuvés pour un usage professionnel (BYOD)

2.2.3. Les réseaux de l'entreprise, les plateformes cloud et les services logiciels

2.2.4. L'accès à Internet, les systèmes de messagerie, les espaces de stockage partagés et les applications métier

2.3. La présente politique s'applique à tous les environnements de travail — sur site, à distance ou hybrides — et pendant toutes les heures d'activité.

3. Objectifs

3.1. Définir ce qui constitue une utilisation acceptable et non acceptable des systèmes informatiques.

3.1.1. Réduire les risques de sécurité liés à un usage abusif, à un accès non autorisé ou à l'introduction de logiciels malveillants.

3.1.2. Protéger les données de l'entreprise, les informations des clients et la réputation de l'entreprise.

3.1.3. Établir des règles opposables et renforcer la responsabilisation de tous les utilisateurs.

3.1.4. Soutenir la surveillance et la conformité afin de détecter rapidement les violations et de mettre en œuvre des mesures correctives.

4. Rôles et responsabilités

4.1. Direction générale

4.1.1. Approuve la présente politique et veille à ce que les ressources et le niveau d'autorité nécessaires à son application soient disponibles.

4.1.2. Examine et approuve toute dérogation à la présente politique.

4.2. Responsable informatique ou prestataire informatique externe

4.2.1. Tient à jour l'inventaire des logiciels et matériels approuvés.

4.2.2. Configure les équipements de manière à faire appliquer les règles d'utilisation acceptable (par exemple : filtrage de contenu, journalisation des accès).

4.2.3. Surveille les usages afin de détecter d'éventuelles violations et mène les investigations nécessaires sur les incidents.

4.2.4. Veille à ce que les équipements personnels (BYOD) soient autorisés et sécurisés lorsqu'ils sont utilisés à des fins professionnelles.

[... 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 faire l'objet d'une revue annuelle par le responsable informatique, avec approbation finale de la direction générale, afin de s'assurer qu'elle reste alignée sur les usages technologiques, les risques émergents et les obligations de conformité.

9.2. Déclencheurs de revue intermédiaire

9.2.1. Des revues doivent également être réalisées en réponse aux événements suivants :

9.2.2. Nouveaux systèmes ou nouvelles technologies (par exemple : nouveau service cloud ou nouvelle plateforme de terminaux)

9.2.3. Violations significatives de la politique

9.2.4. Mise à jour des lois ou des clauses contractuelles ayant une incidence sur l'usage des ressources informatiques

9.3. Documentation des changements

9.3.1. Toute mise à jour doit être consignée dans un journal des versions comprenant :

9.3.1.1. Le numéro de version

9.3.1.2. La date de revue

9.3.1.3. Le résumé des modifications

9.3.1.4. L'autorité d'approbation

9.4. Communication de la politique

9.4.1. Les versions révisées de la présente politique doivent être communiquées à tous les utilisateurs concernés. Les employés doivent attester en avoir reçu communication et l'avoir comprise dans le cadre de leurs obligations de sensibilisation à la sécurité.

10. Politiques associées et articulations

10.1. La présente politique s'articule avec plusieurs autres politiques PME afin d'assurer une couverture complète des responsabilités en matière de sécurité :

10.1.1. P4S – Politique de contrôle d'accès : définit l'application technique et procédurale des usages autorisés et des restrictions de comptes.

10.1.2. P8S – Politique de sensibilisation et de formation à la sécurité de l'information : prévoit la formation des utilisateurs sur les limites d'utilisation acceptable et les obligations de signalement.

10.1.3. P9S – Politique de télétravail : encadre l'utilisation des systèmes de l'entreprise hors site ou à domicile.

10.1.4. P17S – Politique de protection des données et de la vie privée : définit les règles de traitement des données à caractère personnel qui recoupent la surveillance de l'utilisation acceptable et le BYOD.

10.1.5. P30S – Politique de réponse aux incidents : encadre les procédures d'investigation et de réponse en cas d'usage abusif ou de violation des règles d'utilisation acceptable.

11. Normes et référentiels de référence

11.1. ISO/IEC 27001

11.1.1. Clause 5.10 – Exige que les organisations définissent et fassent appliquer des règles d'utilisation acceptable des actifs informationnels.

11.2. ISO/IEC 27002

11.2.1. Mesure 5.10 – Fournit des lignes directrices sur l'utilisation acceptable des systèmes, y compris les comportements autorisés et interdits.

11.3. NIST SP 800-53 Rév. 5

11.3.1. AC-19 – Traite du contrôle de l'utilisation des systèmes, y compris des équipements personnels.

11.3.2. AC-20 – Exige l'autorisation et la surveillance des systèmes externes.

11.3.3. AT-2 – Met l'accent sur la formation des utilisateurs aux pratiques d'utilisation acceptable.

11.4. RGPD de l'UE

11.4.1. Article 5(1)(f) – Exige l'intégrité et la confidentialité des données à caractère personnel, qui peuvent être compromises par un usage abusif de la part des utilisateurs.

11.4.2. Article 32 – Impose la mise en œuvre de mesures techniques et organisationnelles pour sécuriser les systèmes et les données.

11.5. NIS2 de l'UE

11.5.1. Article 21(2)(b) – Exige des politiques de sécurité appropriées, y compris des règles d'utilisation acceptable, afin d'atténuer les cybermenaces.

11.6. DORA de l'UE

11.6.1. Article 9 – Exige des politiques de gestion des risques liés aux TIC, incluant des contrôles d'usage et des mécanismes d'application.

11.7. COBIT 2019

11.7.1. DSS05 – Gérer les services de sécurité : met l'accent sur le contrôle du comportement des utilisateurs au moyen de politiques.

11.7.2. BAI08 – Gérer les connaissances : traite de la sensibilisation aux responsabilités prévues par la politique et à l'utilisation acceptable.