					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P27S					Titre du document : **Politique d'utilisation des services cloud**							
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 applicables

Norme/réglementation	Clause/article	Commentaire
ISO/IEC 27001:2022	Clause 8	
ISO/IEC 27002:2022	Mesures 5.23–5.25	
NIST SP 800-53 Rev. 5	AC-20, SC-12, SC-13, SR-5	
RGPD de l'UE	Article 28, 32 et chapitre V	
NIS2 de l'UE	Articles 21(2)(f), 21(2)(i)	
DORA de l'UE	Articles 5(2), 28	
COBIT 2019	DSS01, DSS05 Gestion des services de sécurité, BAI04	

1. Objet

1.1 La présente politique définit les conditions d'utilisation sécurisée des services cloud au sein de l'organisation. Elle impose la protection des données traitées ou stockées dans le cloud, le contrôle des accès et une gestion responsable des risques.

1.2 Elle aide les PME à satisfaire aux obligations légales et aux attentes des clients en matière de protection des informations sensibles, de prévention des fuites de données et de gestion efficace des risques liés au cloud, sans exiger une infrastructure de niveau grande entreprise.

1.3 La présente politique contribue à la certification ISO/IEC 27001, à la conformité au RGPD et à la maîtrise de la chaîne d'approvisionnement au moyen d'une gouvernance cohérente de l'ensemble des services cloud fournis par des tiers.

2. Champ d'application

2.1 La présente politique s'applique à :

2.1.1 tout service cloud utilisé pour stocker, traiter ou transmettre des données de l'entreprise ;

2.1.2 l'ensemble du personnel, des sous-traitants et des prestataires de services utilisant des outils cloud pour le compte de l'organisation ;

2.1.3 l'ensemble des solutions cloud gratuites ou payantes, y compris les plateformes de messagerie, le partage de documents, les outils SaaS, les plateformes de sauvegarde, la visioconférence et les portails clients ;

2.1.4 tout appareil (poste fixe, appareil mobile, tablette) accédant aux informations de l'entreprise via des applications cloud.

2.2 Cela comprend notamment :

2.2.1 Microsoft 365, Google Workspace, Dropbox Business ;

2.2.2 Zoom, Microsoft Teams, Google Meet ;

2.2.3 AWS, Azure, GCP ;

2.2.4 les outils de sauvegarde et de reprise après sinistre dans le cloud ;

2.2.5 les dossiers partagés ou applications utilisés pour la facturation, la gestion de projet ou la communication avec les clients.

3. Objectifs

3.1 Empêcher l'utilisation non autorisée ou à risque élevé de services cloud non approuvés.

3.2 Garantir que les données sensibles ou réglementées stockées dans le cloud sont protégées au moyen de contrôles techniques et organisationnels appropriés.

3.3 Définir clairement les rôles relatifs à l'approbation, à la configuration, à la surveillance et au retrait de service des services cloud.

3.4 Encadrer les flux de données et imposer les obligations applicables en matière de conservation, de suppression et de protection des données pour les informations stockées dans le cloud.

3.5 Réduire la dépendance aux comptes personnels ou aux outils non maîtrisés en imposant l'approbation de tous les systèmes cloud utilisés à des fins professionnelles.

3.6 Respecter les exigences de l'ISO/IEC 27001:2022, du RGPD, de NIS2 et de DORA pour la gestion des dépendances cloud externes.

4. Rôles et responsabilités

4.1 Directeur général (DG)

4.1.1 Approuve l'utilisation de tout nouveau service cloud.

4.1.2 Examine les risques liés aux fournisseurs cloud et aux types de services.

4.1.3 Veille à l'application de la politique et supervise les décisions relatives aux dérogations.

4.2 Prestataire informatique ou support technique

4.2.1 Évalue et met en œuvre la configuration sécurisée des services cloud.

4.2.2 Met en place les comptes, les contrôles d'accès et les sauvegardes.

4.2.3 Surveille la conformité des mots de passe, de l'authentification multifacteur et des paramètres 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 La présente politique doit faire l'objet d'une revue au moins annuelle par le Directeur général, en coordination avec le prestataire informatique.

9.2 Une revue formelle doit également avoir lieu :

9.2.1 après un incident de sécurité lié au cloud (par exemple violation, perte de données) ;

9.2.2 lorsqu'une nouvelle plateforme cloud majeure est introduite ;

9.2.3 si les exigences légales ou réglementaires évoluent (par exemple mises à jour du RGPD, de NIS2 ou de DORA) ;

9.2.4 si les activités de surveillance révèlent un usage inapproprié ou de nouveaux risques.

9.3 Le DG doit veiller à ce que :

9.3.1 le registre des services cloud soit mis à jour avec les nouveaux services ou ceux retirés ;

9.3.2 les exigences juridiques et de protection des données soient toujours respectées ;

9.3.3 toutes les modifications soient communiquées aux utilisateurs et parties prenantes concernés.

9.4 Les versions archivées doivent être conservées de manière sécurisée, et les anciennes versions de la politique doivent être traitées conformément à la P14S – Politique de conservation et d'élimination des données de l'organisation.

10. Politiques associées et articulations

10.1 La présente politique doit être appliquée en articulation avec les politiques de sécurité de l'information suivantes alignées sur les besoins des PME :

10.1.1 P2S – Politique relative aux rôles et responsabilités de gouvernance : définit les responsabilités liées à l'approbation des services cloud et à la gestion des relations avec les prestataires.

10.1.2 P4S – Politique de contrôle d'accès : soutient les pratiques de connexion sécurisée, de gestion des sessions et de révocation requises pour les plateformes cloud.

10.1.3 P14S – Politique de conservation et d'élimination des données : encadre la sauvegarde, la conservation et la suppression des données hébergées dans le cloud conformément aux obligations légales.

10.1.4 P17S – Politique de protection des données et de la vie privée : garantit que toute donnée à caractère personnel stockée dans des services cloud est traitée conformément aux principes du RGPD.

10.1.5 P30S – Politique de réponse aux incidents : fournit des procédures structurées pour répondre aux incidents de sécurité cloud, y compris la collecte des éléments de preuve et la notification externe.

10.2 Ensemble, ces politiques garantissent une utilisation du cloud sécurisée, conforme et résiliente sur le plan opérationnel.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Clause 8.1 – Exige des organisations qu'elles mettent en œuvre des contrôles opérationnels pour le traitement des données, y compris ceux liés aux systèmes basés sur le cloud.

11.2 ISO/IEC 27002

11.2.1 Mesure 5.23 – Implique une gouvernance de l'utilisation des services cloud et des outils SaaS fournis par des tiers.

11.2.2 Mesure 5.24 – Exige une politique d'utilisation du cloud définie et alignée sur les exigences en matière de risque et de conformité réglementaire.

11.2.3 Mesure 5.25 – Exige des organisations qu'elles s'assurent que les mesures de sécurité des environnements cloud répondent aux besoins de l'organisation.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AC-20 – Exige des politiques formelles d'utilisation pour les systèmes externes tels que les services cloud.

11.3.2 SC-12, SC-13 – Traitent du chiffrement des données en transit et des données au repos dans les environnements cloud.

11.3.3 SR-5 – Couvre les contrôles de risque liés au cloud et aux tiers dans la chaîne d'approvisionnement.

11.4 RGPD de l'UE (2016/679)

11.4.1 Article 28 – Exige que les prestataires cloud agissant en qualité de sous-traitants du traitement respectent des obligations contractuelles contraignantes.

11.4.2 Article 32 – Implique des mesures techniques et organisationnelles pour le traitement des données dans le cloud.

11.4.3 Chapitre V – Interdit les transferts internationaux non autorisés de données à caractère personnel stockées dans le cloud.

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

11.5.1 Article 21(2)(f), (i) – Exige des entités essentielles et importantes qu'elles mettent en place des politiques appropriées relatives à la sécurité des services cloud et au contrôle de la chaîne d'approvisionnement.

11.6 DORA de l’UE (2022/2554)

11.6.1 Article 5(2) – Exige des PME financières qu’elles intègrent la sécurité du cloud dans leurs cadres de gestion des risques liés aux TIC.

11.6.2 Article 28 – Établit des règles de supervision des prestataires tiers critiques de services TIC, y compris les fournisseurs cloud.

11.7 COBIT 2019

11.7.1 DSS01 – « Gérer les opérations » traite de l’intégrité opérationnelle des services cloud.

11.7.2 DSS05 Gestion des services de sécurité – inclut des protections et une surveillance spécifiques au cloud.

11.7.3 BAI04 – « Gérer la disponibilité et la capacité » garantit la continuité d’activité et la performance dans les environnements cloud.