					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P27					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

Norme/Réglementation	Clause/Article	Commentaire
ISO/IEC 27001:2022	Clause 8	Exigences relatives à la planification et au contrôle opérationnel du cloud.
ISO/IEC 27002:2022	Mesures 5.23–5.25	Exigences relatives à l'utilisation, à la politique et à la sécurité des services cloud.
NIST SP 800-53 Rev.5	AC-20, SA-9(5), SC-12 à SC-28, SR-5	Utilisation de systèmes externes, exigences contractuelles et techniques, protections cryptographiques, protection de la chaîne d'approvisionnement.
RGPD de l'UE	Articles 28, 32, chapitre V	Exigences applicables aux sous-traitants cloud, sécurité du traitement, transferts de données.
NIS2 de l'UE	Article 21(2)(f, i)	Exigences relatives aux risques liés aux tiers et à la chaîne d'approvisionnement.
DORA de l'UE	Articles 5(2), 28	Supervision des TIC et des tiers (cloud) pour les entités financières.
COBIT 2019	BAI04, DSS01, DSS05	Disponibilité du cloud, opérations, gestion de la sécurité.

1. Objet

1.1 La présente politique établit les exigences obligatoires de l'organisation pour une utilisation sécurisée, conforme et responsable des services cloud selon les modèles de service Infrastructure as a Service (IaaS), Platform as a Service (PaaS) et Software as a Service (SaaS).

1.2 La présente politique vise à garantir que les services cloud sont adoptés et gouvernés de manière à protéger la confidentialité, l'intégrité et la disponibilité des actifs informationnels, tout en respectant les obligations réglementaires, juridiques et contractuelles.

1.3 Elle définit les contrôles permettant de gérer les risques liés au cloud, de protéger les données, de surveiller la conformité des fournisseurs et d'éliminer les usages non autorisés. Elle soutient également l'innovation métier via les plateformes cloud en conciliant sécurité, fiabilité opérationnelle et efficience des coûts.

2. Champ d'application

2.1 La présente politique s'applique à l'ensemble du personnel, aux sous-traitants et prestataires tiers, ainsi qu'aux consultants externes qui provisionnent, configurent, administrent, utilisent ou consultent des services cloud pour le compte de l'organisation.

2.2 Elle s'applique à tous les environnements dans lesquels les données ou charges de travail de l'organisation sont traitées, y compris :

2.2.1 les déploiements cloud publics, privés, hybrides et communautaires ;

2.2.2 tous les modèles de services cloud (IaaS, PaaS, SaaS) ;

2.2.3 les architectures multicloud et fédérées ;

2.2.4 l’utilisation de shadow IT ou de comptes cloud personnels à des fins professionnelles.

2.3 Elle couvre tous les niveaux de classification de l’information et s’applique aux systèmes internes ainsi qu’aux plateformes hébergées par des fournisseurs dans lesquelles des données détenues par l'organisation ou soumises à réglementation sont stockées ou traitées.

3. Objectifs

3.1 Garantir une utilisation sécurisée et cohérente des technologies cloud au moyen de règles d’usage clairement définies, de configurations de référence de sécurité et de rôles de gouvernance.

3.2 Réduire au minimum les risques opérationnels et réglementaires associés au cloud, y compris l’accès non autorisé, les violations de données, les erreurs de configuration, la non-conformité et l’interruption de service.

3.3 Imposer des exigences de sécurité et de protection de la vie privée à l’ensemble des fournisseurs cloud et en vérifier la conformité au moyen de clauses contractuelles, d’évaluations et de droits d’audit.

3.4 Permettre une adoption du cloud évolutive et résiliente sans compromettre le niveau de sécurité, les exigences juridiques ou la continuité d’activité.

3.5 Aligner la gouvernance et l’utilisation du cloud sur le cadre du SMSI de l'organisation, les obligations juridiques (par exemple, RGPD, DORA), les lignes directrices sectorielles et les bonnes pratiques reconnues du secteur (par exemple, NIST, COBIT).

4. Rôles et responsabilités

4.1 Haute direction

4.1.1 Approuve la Politique d’utilisation du cloud et la feuille de route stratégique d’adoption du cloud.

4.1.2 Examine et valide les dérogations à haut risque aux exigences standard de gouvernance du cloud.

4.1.3 Veille à ce que les initiatives cloud bénéficient d’un financement, d’une supervision et d’une intégration adéquats dans les cadres de gestion des risques de l'organisation.

4.2 Responsable de la sécurité des systèmes d'information (RSSI)

4.2.1 Est responsable de la présente politique et du registre organisationnel des services cloud.

4.2.2 Approuve l’intégration de nouveaux fournisseurs cloud sur la base des diligences préalables et de l’évaluation des risques.

4.2.3 Examine la documentation de conformité des fournisseurs et valide leur alignement en matière 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. ...]

9.1 La présente politique doit être revue au moins une fois par an et mise à jour si nécessaire afin de maintenir son alignement avec :

9.1.1 l’évolution des exigences juridiques et réglementaires (par exemple, RGPD, NIS2, DORA) ;

9.1.2 les évolutions des normes ISO/IEC 27001 ou ISO/IEC 27002 ;

9.1.3 les mises à jour de l’architecture cloud, du paysage des risques ou du portefeuille de services de l'organisation ;

9.1.4 les investigations sur incident, les résultats d’audit ou les enseignements tirés de l’exploitation opérationnelle.

9.2 Le RSSI est chargé d’initier la revue et de réunir les parties prenantes concernées, notamment :

9.2.1 l’architecte sécurité cloud ;

9.2.2 l’équipe juridique et conformité ;

9.2.3 les achats et les gestionnaires de fournisseurs ;

9.2.4 les responsables de service et les opérations informatiques.

9.3 Toutes les mises à jour doivent être :

9.3.1 soumises à une gestion des versions et datées ;

9.3.2 approuvées par la haute direction ;

9.3.3 communiquées aux parties concernées, y compris aux employés, aux prestataires et aux tiers ;

9.3.4 archivées conformément aux politiques internes de gestion documentaire.

9.4 Des revues intermédiaires peuvent être déclenchées par :

9.4.1 de nouveaux engagements avec des CSP ou des migrations majeures ;

9.4.2 des menaces émergentes visant l’infrastructure cloud ;

9.4.3 des changements significatifs dans les obligations contractuelles, juridiques ou sectorielles.

10. Politiques associées et articulations

10.1 La présente politique est étroitement liée aux politiques internes suivantes et s’articule avec elles :

10.1.1 P1 – Politique de sécurité de l’information : établit les principes généraux encadrant le fonctionnement sécurisé des systèmes et des services, que la présente politique applique dans le contexte du cloud.

10.1.2 P5 – Politique de gestion des changements : tous les changements de configuration cloud doivent suivre les procédures de contrôle des changements définies dans la P5.

10.1.3 P13 – Politique de classification et d’étiquetage des données : détermine la manière dont les données sont évaluées avant leur transfert vers le cloud et comment des contrôles tels que le chiffrement et la localisation sont appliqués.

10.1.4 P18 – Politique sur les contrôles cryptographiques : fournit les normes relatives au chiffrement, à la gestion des clés et à l’utilisation des algorithmes cryptographiques, directement appliquées aux configurations des services cloud.

10.1.5 P22 – Politique de journalisation et de surveillance : précise les exigences relatives à la collecte, à la conservation et à l’analyse des journaux qui doivent être appliquées dans les environnements cloud.

10.1.6 P30 – Politique de réponse aux incidents : définit les procédures d’escalade, de confinement et de remédiation pour les événements de sécurité liés au cloud.

10.1.7 P33 – Politique d’audit et de surveillance de la conformité : soutient la préparation à l’audit et l’assurance continue que les contrôles cloud sont appliqués et surveillés.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001 : clause 8.1 – planification et contrôle opérationnels : impose aux organisations de mettre en œuvre et de maîtriser les processus nécessaires pour satisfaire aux exigences de sécurité de l’information, y compris celles impliquant des environnements cloud.

11.2 ISO/IEC 27002:2022 – mesures 5.23 à 5.25 :

11.2.1 annexe A, mesure 5.23 – utilisation des services cloud : impose une évaluation fondée sur les risques, une autorisation formelle et la documentation de l’utilisation des services cloud.

11.2.2 annexe A, mesure 5.24 – politique d’utilisation du cloud : exige l’établissement et l’application de politiques formelles d’utilisation du cloud alignées sur les besoins et les risques de l'organisation.

11.2.3 annexe A, mesure 5.25 – sécurité des services cloud : impose l'intégration de la sécurité, les protections contractuelles et la surveillance des charges de travail et des données hébergées dans le cloud.

11.3 NIST SP 800-53 Rev.5 :

11.3.1 AC-20 – utilisation de systèmes externes : impose des règles et conditions définies pour l'accès aux ressources de l'organisation à partir de systèmes externes ou basés sur le cloud.

11.3.2 SA-9(5) – services de systèmes d'information externes : impose des exigences contractuelles de sécurité, une supervision et une surveillance continue pour les systèmes cloud de tiers.

11.3.3 SC-12 à SC-28 – protections cryptographiques, protection des frontières et intégrité des transmissions : s'alignent sur les exigences de chiffrement, d'identité et d'accès applicables aux services hébergés dans le cloud et aux données en transit.

11.3.4 SR-5 – protection de la chaîne d'approvisionnement : soutient l'évaluation et l'encadrement contractuel des CSP intervenant dans la fourniture des services.

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

11.4.1 article 28 – obligations du sous-traitant : impose des contrats formels avec les fournisseurs cloud afin de garantir la sécurité, la confidentialité et l'auditabilité du traitement des données à caractère personnel.

11.4.2 article 32 – sécurité du traitement : soutient l'application du chiffrement, des contrôles d'accès, de la journalisation et d'autres mesures de protection dans les environnements cloud.

11.4.3 chapitre V – transferts internationaux de données : impose le transfert licite des données en dehors de l'UE/EEE au moyen de garanties telles que les clauses contractuelles types (CCT) ou les décisions d'adéquation.

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

11.5.1 article 21(2)(f, i) : impose aux entités de gérer les risques provenant des fournisseurs tiers de services cloud et d'assurer l'intégrité numérique de la chaîne d'approvisionnement au moyen de mesures contractuelles et techniques.

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

11.6.1 article 5(2) – gouvernance des risques liés aux TIC : impose l'intégration du risque lié aux tiers TIC, y compris les services cloud, dans la gouvernance globale des risques.

11.6.2 article 28 – supervision des prestataires tiers critiques de services TIC : impose aux entités financières de surveiller, maîtriser et rendre compte des dépendances aux fournisseurs cloud, de leur niveau de sécurité et de leur résilience.

11.7 COBIT 2019 :

11.7.1 BAI04 – gérer la disponibilité et la capacité : garantit que les services cloud sont résilients, surveillés et satisfont aux critères de performance définis.

11.7.2 DSS01 – gérer les opérations : soutient l'intégration opérationnelle, la gestion des incidents et les configurations de référence sur les plateformes hébergées dans le cloud.

11.7.3 DSS05 – gérer les services de sécurité : oriente la mise en œuvre de contrôles de sécurité spécifiques au cloud, la surveillance et la prévention des incidents sur les services numériques.