					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P29S					Titre du document : **Politique relative aux données de test et aux environnements de test**							
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	Articles 6.1, 8	
ISO/IEC 27002:2022	Mesures 8.28–8.29	
NIST SP 800-53 Rev. 5	SA-11, SA-12, SC-32	
RGPD de l'UE	Articles 5(1)(c), 25, 32	
NIS2 de l'UE	Article 21(2)(e), (h)	
DORA de l'UE	Article 9	
COBIT 2019	BAI07, DSS05	

1. Objet

1.1 La présente politique définit les exigences de gestion des données de test et des environnements de test afin de prévenir toute exposition accidentelle, toute violation de données ou toute perturbation opérationnelle pendant les activités de test.

1.2 Elle exige que les données réelles des clients ne soient jamais utilisées de manière inappropriée lors des tests de logiciels ou de systèmes et que les environnements de test soient séparés des systèmes de production sur les plans logique et technique.

1.3 La présente politique vise à aider les PME à respecter les exigences de certification ISO/IEC 27001 et les obligations légales applicables en matière de protection des données, tout en restant praticable et opposable pour les organisations ne disposant pas d'une équipe informatique dédiée.

2. Champ d’application

2.1 Cette politique s'applique à :

2.1.1 Tous les environnements de test (par exemple, serveurs de préproduction, environnements de type bac à sable, plateformes de test de développement)

2.1.2 Toutes les données de test, qu'elles soient créées manuellement, générées ou dérivées de systèmes de production

2.1.3 L'ensemble du personnel impliqué dans les activités de test, y compris les employés, les prestataires, les travailleurs indépendants et les prestataires informatiques

2.1.4 Tout test susceptible d'affecter les plateformes orientées client, les applications métier internes ou les services tiers

2.2 Elle couvre à la fois les environnements techniques et les processus utilisés pour prendre en charge :

2.2.1 Le développement de sites web, d'applications et d'outils

2.2.2 Les mises à niveau des systèmes, les tests de configuration et les tests d'intégration

2.2.3 Les tests fonctionnels ou de sécurité, automatisés et manuels

3. Objectifs

3.1 Empêcher l'utilisation de données clients réelles et identifiables dans les tests, sauf si elles sont anonymisées et explicitement approuvées.

3.2 Maintenir une séparation stricte entre les systèmes de test et les systèmes de production afin d'éviter toute exposition involontaire de données ou toute interférence opérationnelle.

3.3 Protéger les systèmes de test et les données de test contre tout accès non autorisé, toute divulgation accidentelle ou toute réutilisation entre environnements sans contrôles appropriés.

3.4 Respecter les réglementations applicables en matière de protection des données (par exemple, RGPD, NIS2) en garantissant que toutes les données de test sont traitées de manière licite, loyale et sécurisée.

3.5 Soutenir la préparation de l'organisation aux audits externes et à la certification ISO/IEC 27001 en documentant les pratiques de test et en imposant des mesures de protection cohérentes.

4. Rôles et responsabilités

4.1 Directeur général (DG)

4.1.1 Assume la responsabilité globale de la protection des données de test et de la sécurité des systèmes de test.

4.1.2 Approuve toute utilisation de données réelles dans les tests après vérification de la mise en œuvre de mesures de protection appropriées (par exemple, anonymisation ou masquage des données).

4.1.3 Vérifie que les activités de test sont correctement documentées et conformes à la présente politique.

4.2 Chef de projet

4.2.1 Coordonne la conception et l'exécution des processus de test.

4.2.2 Veille à ce que tous les membres de l'équipe comprennent et appliquent la présente politique.

4.2.3 S'assure que les systèmes de test sont configurés de manière sécurisée avant le début des tests.

4.2.4 Signale au DG tout incident concernant les environnements de test ou toute fuite de données.

[... 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 Revues planifiées

9.1.1 La présente politique doit faire l'objet d'une revue au moins une fois par an par le directeur général (DG). Cette revue vise à garantir que la politique reste à jour au regard :

9.1.1.1 Des évolutions des outils, plateformes ou environnements de développement logiciel

9.1.1.2 Des obligations légales mises à jour, y compris les exigences relatives à la protection des données ou à la résilience numérique

9.1.1.3 Des exigences de certification des PME et de la préparation à l'audit au titre de l'ISO/IEC 27001

9.2 Déclencheurs de revue intermédiaire

9.2.1 Des revues supplémentaires doivent être réalisées à la suite de :

9.2.1.1 Tout incident impliquant une exposition ou une compromission de données dans les environnements de test

9.2.1.2 L'utilisation de données réelles dans les tests, même si elles sont anonymisées

9.2.1.3 L'introduction de nouvelles méthodes de test, de nouveaux systèmes ou de nouveaux fournisseurs

9.2.1.4 Toute évolution réglementaire affectant la manière dont les données sont traitées pendant les tests

9.3 Gestion des changements et communication

9.3.1 Le DG est responsable de :

9.3.1.1 La mise à jour de la présente politique et de la documentation de toute modification dans l'historique des versions

9.3.1.2 L'information du personnel, des développeurs et des prestataires de services concernés concernant les mises à jour

9.3.1.3 La confirmation que toutes les personnes concernées par les tests comprennent et appliquent les règles les plus récentes

9.3.1.4 Le maintien d'une version accessible de la politique la plus récente à des fins de revue et d'audit

9.4 Audit et documentation

9.4.1 Les enregistrements de toutes les revues de la politique, des approbations d'utilisation de données réelles et de toute justification d'exception doivent être :

9.4.1.1 Conservés de manière sécurisée à des fins d'audit

9.4.1.2 Disponibles sur demande lors des audits internes ou des audits réalisés par des tiers

9.4.1.3 Revus annuellement afin de garantir leur cohérence avec les pratiques de test

10. Politiques associées et articulations

10.1 La présente politique doit être appliquée en articulation avec les politiques PME suivantes afin de maintenir la sécurité et la conformité pendant les tests :

10.1.1 P2S – Politique relative aux rôles et responsabilités de gouvernance : définit les responsabilités en matière de supervision du développement, des tests et de la séparation des systèmes.

10.1.2 P4S – Politique de contrôle d'accès : encadre l'attribution, la gestion et la suppression des identifiants d'accès aux systèmes de test.

10.1.3 P8S – Politique de sensibilisation et de formation à la sécurité de l'information : veille à ce que le personnel comprenne les risques liés aux données de test, les pratiques de traitement sécurisé de l'information et la séparation appropriée des environnements.

10.1.4 P13S – Politique de classification et d'étiquetage des données : soutient une classification claire des données de test et oriente les stratégies d'anonymisation ou de masquage des données.

10.1.5 P17S – Politique de protection des données et de la vie privée : s'aligne sur les obligations du RGPD, y compris les mesures de protection entourant le traitement et le stockage des données à caractère personnel, y compris dans les environnements de test.

10.1.6 P24S – Politique de développement sécurisé : précise les attentes générales de sécurité pour les équipes de développement, y compris l'utilisation sécurisée des données pendant les phases de test.

10.1.7 P30S – Politique de réponse aux incidents : décrit la manière de répondre à toute violation ou à tout problème détecté dans un environnement de test ou causé par un traitement inapproprié des données de test.

10.2 Ces politiques forment un cadre de sécurité cohérent visant à garantir l'intégrité des tests, la minimisation des données et l'alignement complet sur l'ISO/IEC 27001 dans l'ensemble des opérations de développement et d'assurance qualité.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Article 6.1 – Exige des actions d'évaluation et de traitement des risques, y compris pour les risques liés aux tests.

11.1.2 Article 8.1 – Exige la planification et la maîtrise des processus opérationnels, y compris des environnements de mise en œuvre des systèmes de test.

11.2 ISO/IEC 27002

11.2.1 Mesure 8.28 – Exige des organisations qu'elles protègent les données de test et veillent à ce qu'elles ne contiennent pas de données sensibles ni de données réelles issues de la production.

11.2.2 Mesure 8.29 – Exige une séparation claire entre les environnements de développement, de test et de production.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-11 – Couvre les exigences de contrôle applicables au développement et aux tests.

11.3.2 SA-12 – Traite des risques liés aux tests dans la chaîne d'approvisionnement et des évaluations de sécurité.

11.3.3 SC-32 – Exige la séparation des environnements ainsi que des protections pour la confidentialité et l'intégrité des données de test.

11.4 Règlement général sur la protection des données (RGPD) de l'UE

11.4.1 Article 5(1)(c) – Implique la minimisation des données, y compris l'utilisation exclusive des données nécessaires aux tests.

11.4.2 Article 25 – Exige la protection de la vie privée dès la conception, ce qui inclut les contrôles applicables aux environnements de test.

11.4.3 Article 32 – Implique un traitement sécurisé des données à caractère personnel dans tous les systèmes, y compris les environnements hors production.

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

11.5.1 Article 21(2)(e, h) – Exige un développement sécurisé et des tests système sécurisés, en particulier lorsque des services numériques sont exposés à un cyberrisque.

11.6 DORA de l'UE (2022/2554)

11.6.1 Article 9 – Souligne l'importance de la résilience opérationnelle numérique, y compris les tests sécurisés des systèmes TIC par les PME du secteur financier.

11.7 COBIT 2019

11.7.1 BAI07 – Gérer l'acceptation du changement et la transition : comprend des contrôles de test permettant de valider les nouveaux systèmes et le traitement des données.

11.7.2 DSS05 – Gestion des services de sécurité : implique des pratiques de test et de développement qui empêchent l'usage abusif ou l'exposition des données métier.