					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P29					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	Clause 8	Pertinente pour la planification et le contrôle sécurisés des données de test et des environnements de test
ISO/IEC 27002:2022	Contrôles 8.28–8.29	Couvre la sécurisation des données de test et la protection des environnements de test
NIST SP 800-53 Rev.5	SA-11, SC-28, SC-32	Traite des tests et évaluations réalisés par les développeurs, de la protection des données au repos et de l'intégrité
RGPD de l'UE	Articles 5, 25, 32	Couvre la minimisation des données, la protection des données dès la conception et la sécurité du traitement dans les contextes de test
NIS2 de l'UE	Article 21(2)(e), (h)	Porte sur les pratiques sécurisées de développement et de test
DORA de l'UE	Article 9	Porte sur les systèmes TIC, les protocoles et la sécurité des données de test
COBIT 2019	DSS05, BAI07	Traite de la gestion des services de sécurité et de l'acceptation du changement/de la transition

1. Objet

1.1. La présente politique définit les exigences obligatoires applicables à la gestion des environnements de test et des données de test afin d'assurer la sécurité, la confidentialité et l'intégrité opérationnelle tout au long du cycle de développement logiciel et de test.

1.2. Elle vise à prévenir les accès non autorisés, les fuites de données et la contamination des systèmes de production résultant d'environnements de test mal gérés ou de l'utilisation de données réelles dans les activités de test.

1.3. La politique impose le traitement sécurisé des informations utilisées à des fins de test, le durcissement de l'infrastructure de test et la mise en œuvre d'un contrôle d'accès fondé sur les rôles (RBAC), en conformité avec les obligations réglementaires et contractuelles applicables.

2. Champ d'application

2.1. La présente politique s'applique à tous les environnements de test, données, outils et processus utilisés pour les tests de logiciels, de systèmes, d'applications et d'infrastructures au sein de l'organisation.

2.2. Elle couvre :

2.2.1. Les environnements de test provisionnés sur site, dans le cloud ou via des plateformes tierces

2.2.2. Les données de test utilisées dans les tests fonctionnels, de performance, de non-régression et de sécurité

2.2.3. Les activités de test manuelles, scriptées ou automatisées (par exemple, les pipelines CI/CD)

2.2.4. L'ensemble du personnel impliqué dans les activités de test, y compris les équipes internes, les fournisseurs et les prestataires

2.3. La politique s'applique indépendamment de la criticité du système, du type d'application ou du caractère interne ou externalisé du développement.

3. Objectifs

3.1. Prévenir l'utilisation, dans les environnements de test, de données de production, de données sensibles ou de données réglementées (par exemple, PII, données de titulaires de carte), sauf si elles sont anonymisées ou font l'objet d'une approbation spécifique.

3.2. Garantir une séparation complète des réseaux et des accès entre les environnements de test et de production afin d'éviter tout accès non autorisé aux données ou toute contamination des systèmes.

3.3. Exiger le chiffrement, le masquage des données ou la génération de données synthétiques lorsqu'il est nécessaire de disposer de données représentatives à des fins de test.

3.4. Réduire la probabilité de défaillances de conformité, d'exposition des données clients ou de perturbations opérationnelles résultant de données de test ou d'environnements non sécurisés.

3.5. Aligner le traitement des données de test sur les normes du secteur (ISO, NIST, COBIT) et sur les réglementations telles que le RGPD, NIS2 et DORA.

4. Rôles et responsabilités

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

4.1.1. Est propriétaire de la présente politique et impose les mesures de protection techniques et organisationnelles applicables aux données de test et aux environnements de test.

4.1.2. Approuve l'utilisation de données réelles ou sensibles dans les tests, sous réserve d'une justification appropriée et de contrôles compensatoires.

4.2. Responsables QA/Test

4.2.1. Coordonnent la planification des tests et veillent à ce que toutes les activités de test respectent les exigences de la présente politique.

4.2.2. Valident la séparation appropriée des environnements, les accès et la préparation des données pour chaque phase de test.

[... 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 annuelle et être mise à jour si nécessaire pour tenir compte :

9.1.1. Des évolutions des exigences réglementaires (par exemple, RGPD, DORA, NIS2)

9.1.2. De l'adoption de nouveaux outils, plateformes ou pipelines d'automatisation des tests

9.1.3. Des constats d'audit interne ou des recommandations issues des revues post-incident

9.1.4. De l'évolution des processus de développement ou de QA modifiant le traitement des données de test ou l'utilisation des environnements

9.2. Le RSSI est responsable du lancement de la revue en collaboration avec :

9.2.1. Les responsables QA/Test

9.2.2. Les responsables DevOps et infrastructure

9.2.3. Les équipes de développement applicatif

9.2.4. Le délégué à la protection des données (DPO) et la direction juridique

9.3. Toute révision doit être :

9.3.1. Soumise à gestion de versions et conservée dans le référentiel documentaire central

9.3.2. Communiquée au personnel concerné par des canaux formels (par exemple, notifications du SMSI, réunions d'information d'équipe)

9.3.3. Alignée avec les mises à jour des normes techniques, contrôles et procédures opérationnelles associées

9.4. Des revues intermédiaires déclenchées par un événement doivent être menées immédiatement à la suite de tout :

9.4.1. Fuite de données ou incident impliquant des environnements de test

9.4.2. Non-conformité d'audit liée au traitement des données de test

9.4.3. Changement significatif des obligations légales ou de l'architecture informatique

10. Politiques associées et articulations

10.1. La présente politique est étroitement articulée avec les politiques suivantes afin de garantir un traitement sécurisé et conforme des données de test et des environnements de test :

10.1.1. P1 – Politique de sécurité de l'information : établit les principes de sécurité généraux régissant la protection des données de test et la gestion des environnements.

10.1.2. P5 – Politique de gestion des changements : s'applique à la création, à la mise à jour et à la mise hors service des environnements de test ainsi qu'aux pipelines de déploiement.

10.1.3. P13 – Politique de classification et d'étiquetage des données : oriente la sélection des données de test et l'application des contrôles selon le niveau de sensibilité.

10.1.4. P14 – Politique de conservation et d'élimination des données : définit les durées de conservation et les exigences d'élimination sécurisée applicables aux jeux de données de test.

10.1.5. P15 – Politique de sauvegarde et de restauration : impose les pratiques de sauvegarde et la validation de la restauration pour les environnements de test.

10.1.6. P18 – Politique sur les contrôles cryptographiques : précise les normes de chiffrement obligatoires pour les données au repos et les données en transit au sein des plateformes de test.

10.1.7. P22 – Politique de journalisation et de surveillance : encadre la visibilité et la détection d'anomalies pour les activités des environnements de test.

10.1.8. P30 – Politique de réponse aux incidents : définit l'escalade et la remédiation applicables aux violations ou incidents impliquant des systèmes de test.

10.1.9. P33 – Politique d'audit et de surveillance de la conformité : permet de valider le respect de la politique et l'assurance continue.

11. Normes et référentiels de référence

11.1. La présente politique s'aligne sur les normes internationales de cybersécurité et les référentiels réglementaires imposant le traitement sécurisé des données de test et la protection des environnements hors production.

11.2. ISO/IEC 27001 :

11.2.1. Clause 8.1 - impose une planification et un contrôle sécurisés des données de test et des environnements de test.

11.3. ISO/IEC 27002:2022 – Contrôles 8.28–8.29 :

11.3.1. Annexe A, contrôle 8.28 – Données de test sécurisées : exige la protection des données de test utilisées pendant les phases de développement et de test au moyen de l'anonymisation, du masquage des données ou de la génération de données synthétiques.

11.3.2. Annexe A, contrôle 8.29 – Protection des environnements de test : exige la séparation d'avec la production, des contrôles d'accès et le durcissement des environnements pour les systèmes de test.

11.3.3. Ces contrôles définissent les exigences relatives à la gestion sécurisée des données utilisées pendant les tests et à la protection des systèmes hors production contre l'usage abusif, la compromission ou la contamination.

11.4. NIST SP 800-53 Rev.5 :

11.4.1. SA-11 – Tests et évaluation par les développeurs : établit les attentes relatives à des procédures de test sécurisées et reproductibles assorties de contrôles de données appropriés.

11.4.2. SC-28 – Protection des informations au repos : s'aligne sur le chiffrement des données de test stockées dans des systèmes hors production.

11.4.3. SC-32 – Intégrité de l'information : prend en charge la validation des données, la prévention de la corruption et les contrôles d'entrée/sortie pendant les tests.

11.5. RGPD de l'UE (2016/679) :

11.5.1. Article 5 – Minimisation des données : interdit l'utilisation non nécessaire de données à caractère personnel dans les tests.

11.5.2. Article 25 – Protection des données dès la conception : exige l'application de techniques de protection des données dès le début du cycle de développement et de test.

11.5.3. Article 32 – Sécurité du traitement : impose des mesures de protection pour les environnements de test traitant des données à caractère personnel ou des données sensibles.

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

11.6.1. Article 21(2)(e, h) : exige des processus sécurisés de développement et de test logiciel, en mettant l'accent sur la protection contre les accès non autorisés et les fuites de données.

11.7. DORA de l'UE (2022/2554) :

11.7.1. Article 9 – Systèmes TIC et protocoles : exige que les processus de test contribuent à la résilience et protègent les données opérationnelles contre la compromission ou la divulgation non autorisée.

11.8. COBIT 2019 :

11.8.1. DSS05 Gestion des services de sécurité : soutient l'application des politiques de sécurité dans tous les environnements, y compris hors production.

11.8.2. BAI07 – Gérer l'acceptation du changement et la transition : couvre le processus formel de transition du test vers la production, y compris les contrôles sur les données et les environnements.