					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P35S					Titre du document : **Politique de sécurité IoT / OT P35S**							
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, 6.2, 8	
ISO/IEC 27002:2022	Mesures 5.23, 5.31	
NIST SP 800-53 Rev.5	SI-7, CM-7, AC-6, PE-20, SC-7	
RGPD de l'UE	Article 32	
NIS2 de l'UE	Article 21(2)(a), (d), (f)	
DORA de l'UE	Article 9(2), 10(1)	

1. Objet

1.1. La présente politique définit les règles obligatoires applicables à l'utilisation et à la gestion sécurisées des systèmes de l'Internet des objets (IoT) et des technologies opérationnelles (OT) au sein de l'organisation. Ces dispositifs peuvent inclure des capteurs intelligents, des caméras de sécurité, des machines de production, des contrôleurs CVC ou tout autre système industriel connecté au réseau.

1.2. La présente politique a pour objet de :

1.2.1. protéger les opérations physiques et numériques contre toute perturbation ou manipulation résultant de dispositifs connectés insuffisamment sécurisés

1.2.2. imposer un déploiement, une surveillance et une maintenance sécurisés des systèmes IoT et OT

1.2.3. garantir la conformité à l'ISO/IEC 27001:2022, à la directive NIS2 et aux cadres réglementaires associés

1.2.4. définir des mesures de contrôle pratiques et opposables pour les PME opérant dans des environnements de bureau, d'entrepôt ou de production

2. Champ d'application

2.1. La présente politique s'applique à toute personne intervenant dans la planification, l'installation, la configuration, l'utilisation, le support ou l'élimination de dispositifs IoT ou OT. Cela inclut :

2.1.1. les employés, prestataires ou stagiaires disposant d'un accès physique ou d'un accès à distance aux dispositifs

2.1.2. les fournisseurs tiers ou techniciens de maintenance chargés d'installer ou de maintenir des systèmes connectés

2.1.3. les directeurs généraux ou membres du personnel chargés de la supervision des politiques de sécurité

2.2. La politique couvre :

2.2.1. les dispositifs IoT tels que les serrures intelligentes, les équipements de surveillance, les compteurs intelligents ou les imprimantes

2.2.2. les systèmes de technologies opérationnelles (OT), y compris les automates programmables industriels, les interfaces SCADA ou les passerelles industrielles

2.2.3. les équipements de support, les applications d'administration et les réseaux de communication utilisés par ces systèmes

2.3. La présente politique s’applique à tous les sites de travail : environnements de bureau, sites distants, zones de production et plateformes cloud interfaçant avec ces dispositifs.

3. Objectifs

3.1. Déploiement sécurisé : garantir que tous les systèmes IoT/OT sont configurés de manière sécurisée avant leur mise en service dans l’environnement opérationnel.

3.2. Limitation de l’exposition : empêcher tout accès non autorisé, usage abusif ou prise de contrôle de dispositifs connectés au moyen de contrôles d’accès robustes et d’une segmentation et d’un cloisonnement réseau.

3.3. Surveillance continue : maintenir une visibilité sur les opérations IoT/OT au moyen de la journalisation des activités et de la surveillance des comportements inhabituels.

3.4. Responsabilité des prestataires : garantir que les prestataires tiers appliquent des pratiques sécurisées d’installation, de configuration et de maintenance.

3.5. Conformité réglementaire : démontrer un alignement complet avec les normes applicables telles que l’ISO 27001, le RGPD (si des données à caractère personnel sont collectées) et NIS2 pour la résilience des infrastructures critiques.

4. Rôles et responsabilités

4.1. Directeur général (DG)

4.1.1. porte la responsabilité globale de la sécurité des systèmes IoT et OT

4.1.2. approuve la présente politique et veille à son application dans l’ensemble des zones de travail

4.1.3. vérifie que les fournisseurs et prestataires appliquent des pratiques sécurisées de mise en service et de maintenance

4.1.4. autorise l’accès réseau pour tout système IoT/OT

4.2. Employé désigné ou responsable des opérations (le cas échéant)

4.2.1. supervise l’inventaire, l’emplacement et la configuration des dispositifs IoT/OT

4.2.2. consigne l’emplacement de chaque dispositif, son affectation réseau et sa documentation de support

4.2.3. veille à ce que toute modification (par exemple, mise à jour de micrologiciel ou remplacement de dispositif) soit documentée

[... 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 être revue au moins une fois par an par le DG

9.1.2. La revue doit déterminer si la politique demeure efficace, couvre les types de dispositifs actuels et reste alignée sur les nouveaux risques ou technologies

9.2. Mises à jour déclenchées par un événement

9.2.1. Les mises à jour de la politique doivent également être engagées lorsque :

9.2.2. de nouveaux types de systèmes IoT ou OT sont introduits

9.2.3. les fournisseurs publient des avis de sécurité ou des notifications de fin de vie

9.2.4. un incident ou un audit met en évidence des lacunes dans les mesures de contrôle IoT/OT

9.2.5. de nouvelles lois ou normes imposent des exigences supplémentaires

9.3. Documentation et gestion des versions

9.3.1. Toutes les mises à jour doivent être documentées, y compris la date, le numéro de version et un résumé des modifications

9.3.2. Le DG doit conserver les versions historiques de la politique à des fins d'audit

9.4. Communication des modifications

9.4.1. Toute mise à jour de la politique doit être communiquée à l'ensemble du personnel et des fournisseurs concernés

9.4.2. Les versions mises à jour doivent être accessibles via des dossiers partagés ou des supports imprimés sur les sites d'installation ou dans les centres de contrôle

10. Politiques associées et articulations

10.1. La présente politique doit être mise en œuvre en cohérence avec les politiques PME associées suivantes :

10.1.1. P4S – Politique de contrôle d'accès : impose des contrôles de connexion au niveau des dispositifs, l'utilisation de mots de passe robustes et des procédures d'accès autorisé pour les plateformes IoT et OT

10.1.2. P9S – Politique de télétravail : interdit l'utilisation de l'accès à distance aux tableaux de bord IoT/OT via des canaux non sécurisés ou non approuvés

10.1.3. P17S – Politique de protection des données et de la vie privée : s'applique si des dispositifs IoT (par exemple, des caméras de sécurité) traitent ou enregistrent des données à caractère personnel, afin de garantir la conformité au RGPD

10.1.4. P30S – Politique de réponse aux incidents : définit les procédures de détection, de signalement et de résolution des incidents IoT ou OT, y compris en cas d'altération suspectée ou de défaillance opérationnelle

10.1.5. P36S – Politique relative aux médias sociaux et aux communications externes : garantit qu'aucune information sur les dispositifs ou l'architecture réseau n'est communiquée à l'extérieur sans approbation

10.2. Chaque politique associée renforce l'application et l'usage pratique de la présente politique en fournissant des orientations procédurales ciblées.

11. Normes et référentiels de référence

11.1. ISO/IEC 27001

11.1.1. Article 6.1 – Identification et traitement des risques : exige que les risques liés aux systèmes IoT et OT soient évalués et atténués de manière systématique

11.1.2. Article 8.1 – Planification et maîtrise opérationnelles : garantit une maîtrise opérationnelle sécurisée des dispositifs connectés

11.2. ISO/IEC 27002

11.2.1. Mesure 5.23 – Sécurité de l'information pour l'utilisation des technologies opérationnelles : définit une utilisation sécurisée de l'OT dans les environnements physiques et numériques

11.2.2. Mesure 5.31 – Configuration sécurisée des systèmes d'information : impose des configurations durcies pour les dispositifs IoT/OT et l'évitement des paramètres non sécurisés par défaut

11.3. NIST SP 800-53 Rev.5

11.3.1. SI-7 – Intégrité des logiciels, des micrologiciels et de l'information : exige la validation de l'intégrité des micrologiciels et des mises à jour

11.3.2. CM-7 – Principe de fonctionnalité minimale : les dispositifs ne doivent pas avoir de fonctions inutilisées ou non sécurisées activées

11.3.3. AC-6 – Moindre privilège : l'accès aux dispositifs doit être limité aux seuls utilisateurs autorisés

11.3.4. PE-20 – Surveillance des actifs : surveillance physique et opérationnelle des actifs IoT et OT

11.3.5. SC-7 – Protection des frontières : segmentation et contrôle des communications réseau des systèmes connectés

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

11.4.1. Article 32 – Sécurité du traitement : si des données à caractère personnel sont captées (par exemple, au moyen de caméras de surveillance), l'organisation doit mettre en œuvre des mesures techniques et organisationnelles appropriées afin de sécuriser ce traitement

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

11.5.1. Article 21(2)(a) – mesures de gestion des risques

11.5.2. Article 21(2)(d) – configuration et utilisation sécurisées des dispositifs

11.5.3. Article 21(2)(f) – sécurité de la chaîne d'approvisionnement et des systèmes

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

11.6.1. Article 9(2) – Champ d'application de la gestion des risques liés aux TIC : inclut les dispositifs industriels et les logiciels embarqués utilisés dans des environnements opérationnels

11.6.2. Article 10(1) – Continuité des TIC : exige que les configurations des dispositifs prennent en charge les opérations de résilience et de reprise

11.7. COBIT 2019

11.7.1. DSS01 – Gérer les opérations : s'applique à la supervision des opérations technologiques, y compris des dispositifs physiques

11.7.2. DSS05 – Gérer les services de sécurité : garantit que les systèmes connectés sont correctement surveillés et protégés

11.7.3. APO13 – Gérer la sécurité : renforce les politiques de protection des actifs opérationnels au sein des PME