					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P35					Titre du document : **Politique de sécurité IoT / OT P35**							
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	
ISO/IEC 27002:2022	Contrôles 5.7, 5.23, 5.27, 5.31, 5.36	
NIST SP 800-53 Rev.5	SC-7, SI-4, CM-2, AC-6, PL-8	
RGPD de l'UE	Articles 5, 25, 32	
Directive NIS2 de l'UE	Articles 21, 23	
DORA de l'UE	Articles 9, 10	
COBIT 2019	DSS05.01, BAI09.01, APO13.02	

1. Objet

1.1 La présente politique définit les exigences obligatoires de sécurité de l'information applicables au déploiement, à l'exploitation, à la surveillance et à la mise hors service des systèmes de l'Internet des objets (IoT) et des technologies opérationnelles (OT) au sein de l'organisation.

1.2 Elle impose l'intégration de ces systèmes dans le dispositif global de gestion de la cybersécurité de l'organisation et leur protection contre toute compromission, utilisation abusive ou sabotage opérationnel.

1.3 La politique vise à imposer des mesures techniques, organisationnelles et procédurales robustes afin de protéger les systèmes IoT/OT en interface avec les infrastructures physiques, les processus de production et les environnements critiques pour la sécurité.

1.4 Elle soutient le respect des obligations réglementaires et contractuelles en matière de cybersécurité, de sûreté, de maîtrise environnementale et de continuité d'activité.

2. Champ d'application

2.1 La présente politique s'applique à l'ensemble des systèmes IoT et OT, qu'ils soient détenus par l'entreprise, loués ou fournis par des tiers, utilisés dans les environnements opérationnels, administratifs ou de production de l'organisation.

2.2 Les systèmes couverts comprennent notamment :

2.2.1 les équipements IoT tels que les capteurs environnementaux, les dispositifs de contrôle d'accès, l'éclairage intelligent, les équipements de surveillance et les objets connectés portables

2.2.2 les plateformes OT telles que les automates programmables industriels (API), les systèmes SCADA, les systèmes numériques de contrôle-commande (DCS), les interfaces homme-machine (IHM), les interfaces MES et les contrôleurs de terrain

2.2.3 les réseaux de contrôle industriels ou les actifs connectés au cloud assurant la surveillance des opérations physiques

2.3 La politique couvre :

2.3.1 tous les environnements (sur site, en périphérie, dans le cloud)

2.3.2 l'ensemble des parties prenantes (utilisateurs internes, intégrateurs, fournisseurs tiers, prestataires)

2.3.3 toutes les phases du cycle de vie (conception, approvisionnement, déploiement, exploitation, mise hors service)

3. Objectifs

3.1 Protéger l'infrastructure IoT et OT contre les menaces de cybersécurité internes et externes, y compris les attaques par déni de service, les accès non autorisés, la propagation de rançongiciels et l'altération des micrologiciels.

3.2 Veiller à ce que les plateformes IoT/OT ne deviennent pas des vecteurs d'attaque entre les environnements IT et OT et ne compromettent pas les systèmes critiques pour la sécurité.

3.3 Appliquer les principes de sécurité dès la conception et de défense en profondeur tout au long du cycle de vie de ces technologies.

3.4 Permettre une intégration fiable, sécurisée et auditable des plateformes IoT et OT au centre des opérations de sécurité (SOC) de l'organisation et aux dispositifs de réponse aux incidents.

3.5 Veiller à ce que tous les déploiements soient alignés sur les contrôles de l'ISO/IEC 27001 et les référentiels sectoriels applicables (par exemple IEC 62443, ISO 27019, NIST SP 800-82).

4. Rôles et responsabilités

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

4.1.1 Définit les politiques et normes techniques de cybersécurité applicables à l'IoT et à l'OT

4.1.2 Supervise les évaluations des risques, la validation des mesures de sécurité et la coordination interservices

4.2 Ingénieurs OT / responsables de site et d'usine

4.2.1 Valident les configurations des systèmes OT et veillent au respect de la politique dans les zones de production

4.2.2 Maintiennent les protections physiques et logiques garantissant l'intégrité et la sûreté des environnements OT

[... 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 et être mise à jour en fonction :

9.1.1 des évolutions d'architecture des systèmes OT ou IoT, des fournisseurs ou des plateformes

9.1.2 des mises à jour réglementaires majeures (par exemple révisions de DORA, de NIS2 ou de directives sectorielles)

9.1.3 de l'apparition de nouvelles vulnérabilités ou de nouveaux modes opératoires de menace dans les systèmes de contrôle

9.1.4 des constats issus des audits internes ou externes, des tests d'intrusion ou des exercices de red team

9.2 Le RSSI, le responsable de la sécurité OT et les responsables de département concernés sont chargés d'initier conjointement le processus de revue.

9.3 Des revues intermédiaires doivent être déclenchées après :

9.3.1 tout incident lié à l'IoT/OT entraînant une défaillance système ou une perte de données

9.3.2 l'introduction de nouveaux équipements majeurs, de logiciels de surveillance ou de plateformes de micrologiciel

9.3.3 l'intégration de capacités de calcul en périphérie intelligentes ou d'automatisation renforcée par l'IA au niveau terrain

9.4 Toute modification de la politique doit :

9.4.1 être documentée dans l'historique des versions et le registre des modifications de politique

9.4.2 être communiquée à tous les utilisateurs, fournisseurs et opérateurs IT/OT concernés

9.4.3 être approuvée à nouveau par la direction générale

10. Politiques associées et articulations

10.1 La présente politique s'applique en articulation avec les politiques de sécurité de l'information suivantes, qui en assurent le support :

10.1.1 P1 – Politique de sécurité de l'information : établit les principes fondamentaux de sécurité applicables également à la sécurité des systèmes IoT et OT.

10.1.2 P3 – Politique d'utilisation acceptable : définit les restrictions applicables à l'utilisation d'équipements personnels et non autorisés, y compris dans les environnements opérationnels.

10.1.3 P6 – Politique de gestion des risques : encadre l'évaluation, l'acceptation et l'atténuation des risques liés aux systèmes embarqués et aux systèmes de contrôle.

10.1.4 P12 – Politique de gestion des actifs : garantit que tous les systèmes IoT et OT sont formellement inventoriés et qu'un responsable leur est attribué.

10.1.5 P20 – Politique de protection des terminaux / contre les logiciels malveillants : s'applique aux contrôleurs connectés, aux passerelles intelligentes et aux systèmes en périphérie de production.

10.1.6 P22 – Politique de journalisation et de surveillance : s'étend aux procédures de collecte et de revue des journaux pour les environnements OT.

10.1.7 P30 – Politique de réponse aux incidents : régit directement les modalités d'escalade et de gestion des compromissions, anomalies ou défaillances système liées à l'IoT/OT.

10.1.8 P33 – Politique d'audit et de surveillance de la conformité : prévoit les mécanismes d'assurance permettant de valider la conformité continue à la présente politique.

11. Normes et référentiels de référence

11.1 La présente politique est alignée sur des normes internationales reconnues et des cadres réglementaires visant à garantir la sécurité, la résilience et la conformité des systèmes de l'Internet des objets (IoT) et des technologies opérationnelles (OT) dans les environnements industriels, de production et de l'entreprise.

11.2 ISO/IEC 27002:2022 – Contrôles 5.7, 5.23, 5.27, 5.31, 5.36

11.2.1 Contrôle 5.7 – Renseignement sur les menaces : encadre la surveillance des environnements OT et l'identification des vulnérabilités propres à l'IoT.

11.2.2 Contrôle 5.23 – Sécurité de l'information pour l'utilisation des services cloud : s'applique lorsque des équipements IoT sont interfacés avec des plateformes cloud pour la télémétrie, le contrôle ou l'analyse.

11.2.3 Contrôle 5.27 – Principes d'architecture et d'ingénierie des systèmes sécurisés : régit les principes de sécurité dès la conception pour les systèmes embarqués et les réseaux de contrôle.

11.2.4 Contrôle 5.31 – Sécurité dans les processus de développement et de support : impose la validation des logiciels et micrologiciels, les contrôles sur les correctifs et les exigences applicables aux fournisseurs dans les déploiements OT.

11.2.5 Contrôle 5.36 – Conformité aux exigences légales et contractuelles : garantit la conformité des actifs OT aux exigences de sûreté, environnementales et réglementaires.

11.2.6 Ces contrôles définissent collectivement de bonnes pratiques pour sécuriser les systèmes IoT/OT tout au long de leur cycle de vie, y compris la conception de l'architecture, le déploiement

sécurisé, l'application des correctifs, la détection d'anomalies et la conformité aux exigences sectorielles.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-7 – Protection des frontières : garantit que les réseaux OT sont segmentés et protégés contre les accès non autorisés.

11.3.2 SI-4 – Surveillance du système : impose la mise en place de mécanismes de surveillance continue et de détection des anomalies dans les environnements ICS.

11.3.3 CM-2 – Configuration de référence : impose la maîtrise des configurations et le durcissement des plateformes IoT/OT.

11.3.4 AC-6 – Moindre privilège : s'applique aux accès des utilisateurs et aux interventions à distance des fournisseurs sur les systèmes de contrôle embarqués.

11.3.5 PL-8 – Architectures de sécurité et de protection de la vie privée : régit la planification de l'intégration sécurisée des systèmes, notamment dans les projets de modernisation OT.

11.4 RGPD de l'UE (2016/679)

11.4.1 Article 5 – Principes relatifs au traitement des données à caractère personnel : s'applique aux plateformes IoT traitant des données issues de capteurs ou des données comportementales liées à des personnes.

11.4.2 Article 25 – Protection des données dès la conception et par défaut : impose l'intégration de garanties de protection des données dans la conception des produits IoT et des micrologiciels.

11.4.3 Article 32 – Sécurité du traitement : impose le chiffrement, le contrôle d'accès et des communications sécurisées pour les transmissions de données des équipements intelligents.

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

11.5.1 Articles 21 et 23 : imposent des obligations de sécurité aux entités essentielles et importantes utilisant des systèmes OT. Elles comprennent l'évaluation des risques, la notification des incidents et la validation de la chaîne d'approvisionnement des fournisseurs IoT/OT ainsi que de l'intégrité des micrologiciels.

11.6 DORA de l'UE (2022/2554)

11.6.1 Article 9 – Gestion des risques liés aux TIC : impose l'intégration sécurisée des systèmes embarqués et des technologies OT dans le dispositif de gouvernance des risques liés aux TIC.

11.6.2 Article 10 – Exigences de sécurité des TIC : impose des mesures de protection pour les plateformes OT interconnectées utilisées dans les environnements financiers et les services critiques.

11.7 COBIT 2019

11.7.1 DSS05.01 – Protection contre les logiciels malveillants : comprend la détection et la réponse aux menaces propres aux ICS et aux campagnes malveillantes visant l'IoT.

11.7.2 BAI09.01 – Établir et maintenir les exigences de sécurité : couvre l'approvisionnement sécurisé et l'exploitation des infrastructures intelligentes ou embarquées.

11.7.3 APO13.02 – Établir et maintenir un plan de sécurité de l'information : impose l'inclusion des systèmes OT et de leurs vulnérabilités dans la stratégie globale de cybersécurité de l'entreprise.