Politique de Sécurité des Systèmes d'Information (PSSI)

Centrale nucléaire fictive – *Nuky*

Version : 1.0 — Date : Juin 2025

1. Objectifs de la sécurité

La présente Politique de Sécurité des Systèmes d'Information (PSSI) s'inscrit dans le cadre de la protection globale des actifs numériques et industriels de la centrale nucléaire fictive Nuky. Dans un contexte où les menaces cyber sont en constante évolution et où la réglementation impose des exigences de plus en plus strictes, cette politique vise à structurer une démarche cohérente, complète et adaptée à un environnement critique.

La sécurité du système d'information a pour premier objectif de garantir la disponibilité des services essentiels, en particulier ceux liés à la supervision industrielle, à la gestion des accès et à la continuité des opérations. Toute interruption non planifiée de ces fonctions pourrait entraîner des conséquences importantes, tant sur le plan opérationnel que réglementaire.

Un second objectif est de préserver l'intégrité des systèmes et des données. Cela concerne aussi bien la configuration des équipements OT que les référentiels de sécurité, les scripts automatisés ou les bases de données techniques. L'altération volontaire ou accidentelle de ces éléments peut compromettre la fiabilité des processus industriels.

La confidentialité constitue le troisième pilier de cette politique. Elle concerne notamment les schémas réseau, les configurations sensibles, les comptes privilégiés ou les documents internes relatifs à la sécurité des installations. Toute fuite d'information sur ces sujets exposerait la centrale à des attaques ciblées de type APT, particulièrement redoutées dans le secteur de l'énergie.

La PSSI répond également à un impératif de conformité. En tant qu'Opérateur d'Importance Vitale (OIV), la centrale Nuky est soumise aux directives de l'ANSSI. La politique de sécurité intègre ces contraintes réglementaires tout en s'alignant sur les référentiels tels que l'ISO 27001 ou IEC 62645.

Face à la multiplication des incidents de cybersécurité, elle vise à doter la centrale de mécanismes de défense, de détection et de réponse efficaces, organisés autour d'une gouvernance claire, d'une analyse de risque structurée, de mesures techniques robustes et d'un plan d'amélioration continue.

2. Référentiels et cadre réglementaire

La cybersécurité d'une infrastructure classée OIV ne peut être envisagée sans un ancrage fort dans les textes de loi, les recommandations des autorités compétentes et les normes techniques de référence.

Le socle de cette politique repose sur la norme ISO 27001, qui définit les exigences relatives à un système de management de la sécurité de l'information (SMSI). Elle structure l'approche globale du projet en intégrant les dimensions de gouvernance, de gestion des risques, de contrôles opérationnels et d'amélioration continue. Dans le contexte de la

centrale, cette norme permet notamment d'encadrer la séparation entre les zones IT et OT, la classification des actifs et la définition de politiques documentées et auditées.

La norme IEC 62645 vient renforcer cet encadrement en ciblant plus spécifiquement les installations nucléaires. Conçue pour prévenir, détecter et répondre aux actes de malveillance dirigés contre les systèmes de contrôle-commande des centrales, elle introduit des exigences supplémentaires en matière de cloisonnement des réseaux, de gestion des configurations, de surveillance temps réel et de réponse aux incidents. Cette norme s'inscrit dans la continuité de la 27001, tout en intégrant les spécificités techniques et organisationnelles du monde industriel.

Sur le plan national, le Guide OIV publié par l'ANSSI encadre les obligations propres aux opérateurs d'importance vitale. Ce guide impose notamment la mise en place d'un dispositif de supervision de sécurité, la déclaration des incidents graves dans un délai strict de 24 heures et l'audit régulier des prestataires. Il impose également une démarche rigoureuse d'analyse de risque, de classification des systèmes essentiels et d'élaboration de plans de continuité d'activité.

À ces textes s'ajoutent d'autres références utiles, comme le cadre méthodologique EBIOS Risk Manager, recommandé pour la conduite des analyses de risque dans les secteurs sensibles. Ce dernier est particulièrement adapté à l'environnement hybride IT/OT de la centrale, car il permet de croiser les actifs critiques, les scénarios de menace réalistes et les mesures de sécurité à mettre en œuvre de manière pragmatique.

La PSSI s'inscrit donc dans un cadre structurant, qui articule des normes internationales, recommandations nationales et bonnes pratiques industrielles. Ce socle réglementaire n'est pas figé : il est régulièrement revu à la lumière des évolutions technologiques, des incidents observés dans le secteur et des retours d'expérience internes. Il garantit à la centrale un haut niveau de conformité et une posture de sécurité adaptée aux menaces modernes.

3. Organisation de la sécurité

La mise en œuvre d'une politique de sécurité efficace repose avant tout sur une organisation claire, structurée et stable. La répartition des responsabilités ne peut souffrir d'ambiguïté. La sécurité n'est pas l'affaire d'une seule personne, mais d'un ensemble d'acteurs, coordonnés autour de rôles bien définis.

Au sein de la centrale Nuky, la responsabilité globale de la cybersécurité est confiée au Responsable de la Sécurité des Systèmes d'Information (RSSI). Ce dernier agit en tant que pilote de la démarche SSI, garant de la cohérence des choix techniques et stratégiques, et interlocuteur principal en cas d'incident ou d'audit. Son rôle est transverse : il intervient aussi bien sur les périmètres IT que sur les infrastructures industrielles OT, en coordination avec les équipes concernées.

Pour assurer un suivi opérationnel efficace, deux référents techniques sont désignés : l'un pour le périmètre informatique classique, l'autre pour les systèmes industriels. Ils traduisent localement les orientations du RSSI, veillent à la conformité des déploiements et assurent le lien avec les équipes d'exploitation. Cette dualité permet de prendre en compte les particularités de chaque environnement, tout en assurant une cohérence globale dans l'approche de sécurité.

Un comité de sécurité est mis en place pour valider les grandes orientations, arbitrer les priorités et suivre les incidents majeurs. Il réunit la direction du site, le RSSI, les référents

techniques, et, selon les sujets abordés, les représentants des prestataires ou des fonctions sûreté. Ce comité joue un rôle central dans la gouvernance du système d'information et garantit l'alignement entre les exigences opérationnelles, réglementaires et techniques.

En cas d'incident significatif, une cellule de crise cyber peut être activée. Cette structure ad hoc, définie à l'avance dans le plan de gestion de crise, regroupe les compétences nécessaires à l'analyse, à la décision et à la communication. Les rôles y sont formalisés pour éviter toute improvisation : qui analyse, qui décide, qui informe, qui intervient. Des exercices sont régulièrement organisés pour tester l'efficacité de cette cellule et la capacité de l'organisation à faire face à un événement majeur.

Enfin, un tableau de répartition des responsabilités (type RACI) est utilisé pour formaliser les rôles de chaque acteur sur les processus clés. Ce tableau permet de préciser qui est responsable, qui doit être consulté, qui valide les décisions, et qui doit simplement être informé. Il couvre aussi bien les activités de gestion des accès, de supervision réseau, de formation des utilisateurs que de réponse aux incidents.

Ce cadre organisationnel constitue un socle indispensable pour garantir la réactivité, la cohérence et l'efficacité de la démarche de sécurité. Dans un environnement critique, la cybersécurité est avant tout une affaire d'anticipation, de clarté des rôles et de coordination humaine.

4. Principes fondamentaux

La sécurité de l'information repose avant tout sur des principes solides, appliqués avec rigueur et constance. Ces fondements structurent l'ensemble des mesures techniques, organisationnelles et humaines mises en œuvre. Ils guident les choix stratégiques, orientent les priorités opérationnelles, et assurent une ligne directrice commune pour l'ensemble des acteurs.

Le premier principe est celui du moindre privilège. Chaque utilisateur, chaque service, chaque processus ne dispose que des droits strictement nécessaires à l'exercice de ses fonctions. Ce principe réduit la surface d'attaque en limitant les capacités d'action d'un compte ou d'un composant compromis. Il est appliqué tant aux comptes humains qu'aux comptes de service, y compris dans les environnements OT où les logiques d'accès sont parfois historiquement permissives.

Ensuite, la centrale applique une logique de défense en profondeur. Il ne s'agit pas de compter sur un seul rempart, mais de superposer plusieurs niveaux de protection. Des contrôles physiques, des filtrages réseau, des durcissements systèmes, des restrictions logicielles et des surveillances actives coexistent pour ralentir, détecter ou bloquer une attaque à différentes étapes. Cette approche assure une résilience accrue face aux menaces persistantes.

La traçabilité constitue un autre pilier fondamental. Toutes les actions sensibles sont journalisées de manière horodatée et centralisée. Cette traçabilité s'applique aux accès utilisateurs, aux modifications de configuration, aux connexions réseau et aux anomalies détectées par les outils de supervision. Elle permet une analyse post-incident efficace, facilite les audits, et contribue à une meilleure compréhension des comportements techniques au sein du système.

La séparation stricte entre les zones IT et OT est également un principe structurant. Les flux sont filtrés, contrôlés, surveillés et justifiés. Une DMZ industrielle assure une zone tampon entre les deux mondes, limitant les points de contact. Cette segmentation réduit

considérablement les risques de propagation en cas de compromission et permet une application différenciée des politiques de sécurité selon les contextes.

Enfin, la gestion des accès est encadrée de manière rigoureuse. Tous les comptes sont nominatifs, associés à des profils clairement définis, et régulièrement revus. L'authentification forte est progressivement généralisée, en particulier sur les interfaces sensibles. Un contrôle centralisé permet de réagir rapidement en cas de départ, de changement de fonction ou de suspicion de compromission.

Parmi les mesures transverses essentielles, on peut citer :

- La mise en œuvre du cycle PDCA (Plan – Do – Check – Act) pour garantir l'amélioration continue du système de sécurité.

- La prise en compte systématique des retours d'expérience issus d'incidents réels ou simulés, afin de renforcer les procédures existantes.

Ces principes ne sont pas de simples recommandations : ils sont ancrés dans la réalité de l'exploitation, traduits en procédures concrètes, et régulièrement testés. Ils constituent le socle sur lequel repose la robustesse de l'ensemble du dispositif de sécurité.

5. Protection des systèmes critiques

Assurer la sécurité des systèmes critiques revient à protéger les composants qui, s'ils venaient à être compromis, pourraient perturber gravement l'exploitation, mettre en danger la sûreté ou enfreindre les exigences réglementaires. Il s'agit d'un travail de fond, mené à plusieurs niveaux, sur les plans technique, organisationnel et procédural.

Le processus commence dès l'installation des serveurs et des équipements réseau par une politique systématique de durcissement. Les systèmes d'exploitation, qu'ils soient Linux ou Windows, sont configurés de manière à désactiver tous les services non essentiels, à renforcer les permissions par défaut, à interdire les connexions root directes, et à limiter la surface d'exposition aux seuls flux justifiés. L'environnement est ainsi assaini avant toute mise en production.

Les mises à jour de sécurité sont gérées avec attention. Dans les environnements IT, les correctifs critiques sont appliqués de manière semi-automatisée. Dans les environnements OT, les mises à jour font l'objet d'un cycle rigoureux de test en préproduction, afin de préserver la stabilité des équipements industriels. Aucune modification ne peut être appliquée sans validation préalable lors de créneaux de maintenance encadrés.

Les services critiques tel que DNS, NTP, DHCP, supervision, ou journalisation sont installés localement et configurés pour répondre uniquement aux besoins internes. Ils sont cloisonnés, surveillés, et protégés contre toute sollicitation externe. Par exemple, le serveur DNS interne n'accepte que les requêtes provenant du réseau de gestion, et le service DHCP est restreint aux postes utilisateurs, les équipements industriels disposant d'adresses fixes pour garantir la traçabilité.

Les comptes à privilèges font l'objet d'un encadrement strict. Chaque administrateur dispose d'un double compte : l'un pour les opérations courantes, l'autre pour les tâches sensibles. Les sessions d'administration sont limitées dans le temps, tracées, et soumises à authentification forte. Aucune exception n'est tolérée sur ces principes, qui constituent un rempart contre les abus ou les compromissions latentes.

L’ensemble de l’infrastructure bénéficie d’une supervision centralisée. Un SIEM collecte les journaux de sécurité de tous les systèmes : serveurs, pare-feux, automates, bases de données, services critiques. Les événements sont analysés en temps réel, corrélés à l’aide de règles personnalisées, et visualisés via des tableaux de bord synthétiques. Ce dispositif permet de repérer rapidement les anomalies, les comportements suspects ou les tentatives d’intrusion.

Des tests d’intrusion viennent régulièrement valider l'efficacité des dispositifs en place. Ces tests sont préparés en amont, encadrés par des règles strictes de non-perturbation des systèmes critiques, et réalisés selon une approche en boîte grise. Ils permettent d’identifier les vulnérabilités résiduelles, d’évaluer la robustesse des systèmes exposés, et d’enrichir le plan d’action en continu.

À travers cette approche intégrée, la protection des systèmes critiques ne repose pas uniquement sur des outils, mais sur une stratégie globale cohérente, résiliente et rigoureusement appliquée. Elle vise à garantir que chaque composant, chaque accès, chaque flux est maîtrisé, surveillé et justifiable, en permanence.

6. Gestion des incidents

La survenue d’un incident de sécurité, qu’il s’agisse d’un comportement anormal, d’une compromission avérée ou d’un simple doute sur l’intégrité d’un système, exige une réponse rapide, structurée et proportionnée.

Tout commence par la détection. Celle-ci peut être déclenchée automatiquement par les outils de supervision (SIEM), manuellement par un opérateur, ou à l’occasion d’un audit. Dès qu’un événement suspect est relevé, il est enregistré dans un journal centralisé, accompagné d’un horodatage précis et d’un premier niveau de qualification. L’objectif à ce stade est de déterminer si l’événement relève d’une anomalie bénigne, d’une erreur humaine ou d’un incident nécessitant une réponse formelle.

Lorsqu’un incident est confirmé, une cellule de réponse est immédiatement mobilisée. Celle-ci inclut le RSSI, les référents techniques IT et OT, et, selon la nature du problème, des experts métiers ou des représentants de la direction. Ensemble, ils procèdent à l’analyse de la situation : origine, portée, systèmes impactés, risques de propagation. Des mesures de confinement sont prises le cas échéant : isolement réseau, désactivation d’un service, modification temporaire d’une règle de pare-feu. Ces décisions doivent toujours viser un équilibre entre réactivité et préservation des opérations critiques.

Si l’incident dépasse un certain seuil de gravité (compromission d’un système sensible, perte de disponibilité majeure, suspicion d’intrusion ciblée)la cellule de crise cyber est activée. Ce dispositif renforcé permet d’impliquer directement la direction, le service sûreté, le représentant ANSSI si nécessaire, et d’organiser la communication en interne comme en externe. Dans le cadre réglementaire des OIV, toute atteinte sérieuse à la sécurité doit être déclarée officiellement à l’ANSSI dans un délai de 24 heures.

Une fois le système stabilisé, les actions de remédiation sont engagées. Cela peut inclure la réinitialisation de comptes, le remplacement de composants compromis, l’application de correctifs, ou la mise à jour des signatures de détection. Cette phase est essentielle pour restaurer les services, mais aussi pour prévenir toute récidive ou effet secondaire.

Le processus ne s’arrête pas à la résolution technique. Un retour d’expérience (REX) est systématiquement rédigé et partagé avec les équipes concernées. Il permet d’analyser les

causes profondes, de corriger les faiblesses structurelles, et d'ajuster les procédures. Ce travail contribue directement à l'amélioration continue du dispositif de sécurité.

La gestion des incidents ne se limite donc pas à une réaction ponctuelle, mais s'inscrit dans une véritable stratégie de résilience. Chaque événement traité devient une opportunité d'apprentissage, un levier d'amélioration, et un rappel que dans un environnement critique, l'anticipation et la préparation sont les meilleures protections.

7. Sensibilisation et documentation

Aucune politique de sécurité, aussi complète soit-elle sur le plan technique, ne peut produire ses effets sans l'adhésion active des personnes qui la mettent en œuvre. La sensibilisation des utilisateurs et la qualité de la documentation sont ainsi deux leviers essentiels pour ancrer durablement la cybersécurité dans les pratiques quotidiennes de la centrale Nuky.

La sensibilisation commence dès l'arrivée d'un nouvel intervenant, qu'il soit salarié, prestataire ou stagiaire. Une session d'accueil sécurité lui présente les règles de base, les gestes à proscrire et les comportements attendus. Cette première étape pose les fondations d'une culture commune, où la sécurité n'est pas vécue comme une contrainte mais comme une condition de fonctionnement normale.

Mais au-delà de cette introduction, un effort de formation continue est mené tout au long de l'année. Des rappels réguliers sont diffusés, sous forme de supports courts, visuels et contextualisés. Des ateliers plus techniques sont proposés aux profils exposés : administrateurs système, opérateurs industriels, référents locaux. Ces sessions couvrent des sujets variés : gestion des incidents, manipulation sécurisée de supports amovibles, réaction face à une tentative de phishing, procédures de crise.

Les retours d'expérience issus des simulations ou des incidents réels viennent nourrir cette démarche pédagogique. Un cas concret, anonymisé mais véridique, permet souvent de mieux ancrer les bonnes pratiques qu'un rappel purement théorique. L'objectif est d'ancrer une vigilance diffuse, où chacun sait qu'il a un rôle à jouer, même indirectement, dans la protection du système d'information.

En parallèle, la documentation joue un rôle de socle technique et organisationnel. Toutes les mesures de sécurité mises en œuvre sont accompagnées d'une fiche de configuration détaillée. Celle-ci comprend les paramètres choisis, les justifications associées, les éventuelles dépendances techniques, ainsi que les procédures de retour arrière en cas de besoin. Rien n'est laissé à l'intuition ou à la mémoire individuelle.

Cette documentation est centralisée dans un espace sécurisé, partagé entre le RSSI, les référents IT/OT et les exploitants habilités. Elle est versionnée dans un dépôt Git interne ou un wiki structuré, afin de garantir la traçabilité des évolutions. Toute modification significative d'une règle pare-feu, d'un script automatisé, d'un service critique y est documentée en temps réel.

Parmi les contenus disponibles figurent :

- Les procédures de sauvegarde et de restauration, avec exemples et options avancées.

- Les règles UFW actives sur chaque hôte Linux, accompagnées de leur justification métier.

- Les filtres et alertes configurés dans le SIEM, avec la logique de détection sous-jacente.

- Les conditions d’accès, les plages de maintenance et les règles d’intervention sur les équipements OT.

Enfin, la transmission des savoirs est formalisée dans une procédure de transfert opérationnel. Lorsqu’un projet de sécurité est finalisé, une réunion est organisée entre le RSSI, les référents techniques et les futurs exploitants. Cette séance s’appuie sur des supports visuels, des démonstrations, et donne lieu à des échanges pour valider la bonne appropriation des outils et des processus.

Cette démarche documentaire ne vise pas uniquement à satisfaire les auditeurs. Elle constitue un pilier de la continuité opérationnelle, de l’autonomie des équipes, et de la capacité collective à réagir, comprendre, et corriger lorsqu’un incident se produit.

8. Mise à jour de la politique

La cybersécurité est un domaine en constante évolution. Les menaces changent, les outils se perfectionnent, les exigences réglementaires se renforcent, et les organisations elles-mêmes se transforment. Dans ce contexte, une Politique de Sécurité des Systèmes d’Information ne peut rester figée. Elle doit être vivante, révisée régulièrement, et alignée en permanence sur les réalités techniques et organisationnelles du terrain.

À la centrale Nuky, la PSSI fait l’objet d’une révision au moins une fois par an. Cette révision est menée sous l’autorité du RSSI, en lien avec les référents techniques IT et OT, ainsi qu’avec le comité de sécurité. Elle s’appuie sur les enseignements tirés des audits, des tests d’intrusion, des exercices de gestion de crise, mais aussi sur les retours d’expérience internes ou issus du secteur nucléaire dans son ensemble.

En dehors de cette revue annuelle, des mises à jour ponctuelles peuvent être déclenchées à tout moment lorsqu’un changement significatif intervient. Il peut s’agir de l’introduction d’une nouvelle technologie, de l’évolution du périmètre réglementaire, de la détection d’une faille structurelle ou encore de l’intégration d’un nouveau prestataire critique. La souplesse de cette approche garantit que la politique reste pertinente sans pour autant perdre en stabilité.

Chaque nouvelle version de la PSSI est validée formellement par la direction. Elle est ensuite diffusée à l’ensemble des collaborateurs concernés, accompagnée d’un résumé des changements apportés. Cette communication permet de maintenir une compréhension partagée des règles en vigueur et de s’assurer que les pratiques terrain sont bien alignées avec les intentions stratégiques.

Pour garantir sa traçabilité, chaque version est numérotée, datée et archivée. Les anciennes versions restent accessibles à des fins de comparaison ou d’audit. Lorsqu’un écart est identifié entre la politique et une pratique constatée, une procédure de mise en conformité est enclenchée, avec l’objectif de corriger soit la pratique, soit le texte même de la PSSI.

Enfin, la mise à jour de la politique s’inscrit dans une logique d’amélioration continue. Elle reflète la maturité croissante de l’organisation face aux enjeux de cybersécurité, et traduit concrètement l’ambition collective de faire de la sécurité un pilier durable et partagé.