A Tassec Investment Holdings ' Company

Procédure de gestion des incidents de Scanning Systems

SCANNING SYSTEMS-SGES-PR08 Procédure de gestion des incidents de Scanning Systems

Date d'approbation	
Date d'entrée en vigueur	
Historique de révision	**Première édition : Version A du 17 Septembre 2024** **Version B révisée : 16 Octobre 2024**
Remplacé/modifié	**Version C : 17 Juillet 2025**

Table des matières

1 Introduction

Une procédure de gestion des incidents permet de détecter rapidement les problèmes, d'évaluer leur impact, de coordonner une réponse appropriée et de restaurer les services normaux dans les plus brefs délais. Cette procédure implique une collaboration étroite entre les différents départements, l'utilisation de technologies pour la surveillance et la communication, ainsi qu'une formation régulière du personnel pour assurer une réponse rapide et adéquate aux situations d'urgence. En mettant en place une telle procédure, Scanning Systems peut non seulement minimiser les perturbations, mais aussi renforcer la confiance des usagers et des autorités dans la fiabilité et la sécurité de ses opérations frontalières.

2 Objectifs

Cette procédure permet de :

- Identifier rapidement les incidents ;
- Réagir promptement et efficacement pour minimiser les impacts ;
- Documenter et analyser les incidents pour éviter leur récurrence ;
- Assurer la communication interne et externe appropriée ;
- Garantir la continuité des opérations.

3 Portée

Cette procédure s'applique à tous les employés, sous-traitants et visiteurs présents sur les sites des PCJ.

4 Types d'Incidents

- Incidents de sécurité physique (intrusion, vol, vandalisme, etc.) ;
- Incidents de sécurité informatique (cyberattaque, violation de données, etc.) ;
- Pannes d'équipement ;
- Incidents environnementaux (déversement de produits chimiques, pollution, etc.) ;
- Incidents de santé et sécurité au travail (accidents, maladies, etc.) ;
- Interruption des services (panne de courant, problème de réseau, etc.).

5 Responsabilités

5.1 Responsable HSE

- Coordonner les actions de gestion des incidents ;
- Maintenir à jour la procédure de gestion des incidents ;
- Organiser des formations et des exercices réguliers ;

5.2 Employés

- Connaître et suivre les procédures de gestion des incidents ;

- Signaler immédiatement tout incident ;
- Participer aux formations et exercices.

5.3 CLO : Agents de liaison E&S

- Fournir assistance technique et logistique lors des incidents ;
- Coordonner avec le responsable des incidents.

6 Identification et Signalement

Un contrôle constant des opérations et des infrastructures est assuré par des dispositifs de supervision avancés et des outils de repérage d'incidents. Ces technologies permettent d'identifier rapidement toute irrégularité ou menace, facilitant ainsi une intervention rapide et adaptée.

En parallèle, une communication prompte et exacte des incidents est cruciale pour une gestion optimale. Tout membre du personnel constatant un incident doit le signaler sans délai via les voies de communication prédéfinies, que ce soit par téléphone, courriel ou plateforme de signalement spécifique en ligne. Lors de ce signalement, communiquer des informations précises sur l'incident, notamment sa nature, son emplacement et ses conséquences potentielles, afin de permettre une évaluation rapide et une réponse appropriée. Cette méthodologie rigoureuse assure un traitement efficace de chaque incident, réduisant ainsi les perturbations et renforçant la sûreté des activités frontalières.

7 Réaction et Gestion

7.1 Évaluation Initiale

Lorsqu'un incident est signalé, la première étape consiste à effectuer une évaluation initiale pour déterminer la nature et la gravité de l'incident. Cette évaluation doit être rapide et précise, permettant d'identifier les menaces immédiates, les ressources affectées et les actions prioritaires nécessaires. Le personnel responsable doit évaluer les informations fournies lors du signalement et utiliser des outils de diagnostic pour comprendre l'étendue de l'incident.

7.2 Actions Immédiates

Suite à l'évaluation initiale, des actions immédiates doivent être entreprises pour contenir et atténuer l'impact de l'incident. Ces actions peuvent inclure l'isolation des systèmes affectés, l'activation des protocoles de sécurité, la communication avec les parties prenantes pertinentes et la mobilisation des équipes de réponse aux incidents. L'objectif est de limiter les dommages, de protéger les actifs critiques et de maintenir autant que possible la continuité des opérations. Les actions immédiates doivent être documentées pour une référence ultérieure.

7.3 Enquête et Analyse

Après avoir stabilisé la situation, une enquête approfondie et une analyse de l'incident sont

nécessaires pour comprendre ses causes fondamentales et ses implications. Cette phase implique la collecte et l'examen des preuves, l'analyse des données de surveillance et la conduite d'entretiens avec les personnes concernées. L'objectif est de déterminer comment et pourquoi l'incident s'est produit, d'identifier les vulnérabilités exploitées et de développer des recommandations pour prévenir des incidents similaires à l'avenir. Les résultats de l'enquête doivent être documentés dans un rapport détaillé, qui sera utilisé pour améliorer les procédures et renforcer les mesures de sécurité.

8 Communication

8.1 Interne

- Informer les employés concernés dès qu'un incident est détecté et évalué, il est crucial d'informer immédiatement tous les employés concernés des détails de l'incident et des actions en cours. Cette communication doit inclure des informations sur la nature de l'incident, son impact potentiel sur les opérations et les mesures immédiates prises pour y remédier.
- Assurer une communication régulière : Maintenir une communication continue et régulière avec les employés est essentiel pour garantir que tout le monde reste informé des développements de l'incident. Des mises à jour fréquentes doivent être fournies via des réunions, des courriels ou des systèmes de messagerie internes pour partager les progrès réalisés et les prochaines étapes prévues.

8.2 Externe

- Communiquer avec les services d'urgence et les autorités : En cas d'incident grave nécessitant l'intervention des services d'urgence ou des autorités compétentes, il est impératif de les contacter immédiatement. Fournir des informations claires et détaillées pour permettre une réponse rapide et coordonnée. Collaborer étroitement avec ces services pour assurer la sécurité et la résolution de l'incident.
- Fournir des informations aux parties prenantes externes : Selon la nature de l'incident, il peut être nécessaire de communiquer avec des parties prenantes externes telles que les usagers, les fournisseurs et les partenaires. Fournir des informations pertinentes et précises sur l'incident, son impact et les mesures prises pour le résoudre. Assurer une transparence et une réactivité pour maintenir la confiance et minimiser les inquiétudes externes.

9 Résolution et Reprise

9.1 Résolution

- Mettre en œuvre les actions correctives : Une fois l'incident analysé et les causes identifiées, il est crucial de mettre en œuvre rapidement les actions correctives

nécessaires pour résoudre l'incident. Cela peut inclure des correctifs logiciels, des modifications de configuration, des réparations matérielles ou des mesures organisationnelles. Chaque action doit être soigneusement documentée et exécutée conformément aux procédures établies.

- Vérifier la résolution : Après avoir mis en œuvre les actions correctives, il est essentiel de vérifier que l'incident est complètement résolu. Cela implique des tests rigoureux pour s'assurer que les systèmes et les processus fonctionnent normalement sans anomalies résiduelles. Une fois la résolution confirmée, une communication doit être faite pour informer toutes les parties concernées que l'incident est résolu.

9.2 Reprise des Activités

- Conditions de sécurité et de fonctionnement : Avant de reprendre les opérations normales, il est impératif de s'assurer que toutes les conditions de sécurité et de fonctionnement sont remplies. Cela inclut la vérification de l'intégrité des systèmes, la confirmation que toutes les mesures de sécurité sont en place et fonctionnent correctement, et la garantie que les environnements opérationnels sont stables et sécurisés.
- Vérifications de sécurité et réparations : Effectuer des vérifications de sécurité supplémentaires et, si nécessaire, des réparations pour s'assurer qu'aucune vulnérabilité ne persiste. Cela peut inclure des audits de sécurité, des tests de pénétration ou des évaluations de risque. Toute réparation ou ajustement doit être documenté et validé avant la reprise des activités normales.

10 Documentation et Amélioration

10.1 Documentation

- Conserver tous les documents relatifs aux incidents : Il est essentiel de maintenir des archives complètes de tous les incidents, incluant les rapports initiaux, les enquêtes, les actions correctives et les communications internes et externes. Chaque document doit être daté et signé par les responsables concernés pour garantir la traçabilité et l'authenticité.
- Maintenir une base de données accessible : Une base de données centralisée et accessible des incidents doit être mise en place. Cette base de données permet d'analyser les incidents passés, d'identifier les tendances et de tirer des enseignements précieux pour améliorer les procédures de gestion des incidents. Elle doit être régulièrement mise à jour et sécurisée pour protéger les informations sensibles.

10.2 Amélioration Continue

- Réviser régulièrement la procédure de gestion des incidents : Pour s'assurer que la

gestion des incidents reste efficace et pertinente, il faut revoir et évaluer régulièrement la procédure en place. Cette révision doit tenir compte des nouveaux défis, des retours d'expérience et des évolutions technologiques.

- Intégrer les leçons apprises et les meilleures pratiques : Chaque incident offre une opportunité d'apprentissage. Les leçons tirées des incidents passés doivent être intégrées dans les procédures de gestion des incidents. De plus, les meilleures pratiques de l'industrie doivent être adoptées pour renforcer les capacités de réponse aux incidents.
- Mettre à jour les formations et les équipements : Pour que le personnel soit toujours prêt à réagir efficacement, les programmes de formation doivent être régulièrement mis à jour pour refléter les nouvelles procédures, les nouvelles technologies et les leçons apprises. De plus, les équipements utilisés pour la détection, la gestion et la résolution des incidents doivent être maintenus à jour et en bon état de fonctionnement.
- Mettre à jour cette procédure chaque fois que cela sera nécessaire pour s'assurer qu'elle reste pertinente et conforme aux nouvelles réglementations et aux bonnes pratiques en la matière.