Published version: 2.0

PROCÉDURE DE GESTION DES INCIDENTS

Comme ECS prône la méthode CSR, « ***C***reating ***S***ustainable ***R***eliable logistics » (création d'une logistique durable et fiable), nous nous engageons à fournir un service durable et de haute qualité à nos clients et/ou fournisseurs et nous nous efforçons donc de travailler de manière ouverte et responsable afin d'instaurer la confiance et le respect de toutes nos parties prenantes. Par conséquent, nous aimerions vous informer de notre procédure de gestion des incidents.

Cette procédure vise à garantir qu'en cas d'incident, d'accident ou de presque-accident, un processus uniforme soit mis en place, avec un responsable dédié, pour gérer rapidement l'incident afin de :

- minimiser l'impact ou l'effet de l'incident sur les personnes, la planète et le profit ;
- informer toutes les parties prenantes concernées[1] en temps utile et avec des informations correctes ;
- tirer des leçons précieuses pour l'avenir.

Cette procédure s'applique à tout incident[2] ayant causé des dommages potentiels ou réels aux produits ou à tout incident au cours duquel des problèmes juridiques, de (sécurité) alimentaire et sanitaire, de santé, de qualité et d'environnement, de sécurité informatique ou des situations d'urgence potentielles peuvent survenir ou surviennent.

Procédure formelle d'ECS en cas d'incident :

Incident durant le transport	***Définition d'un incident :*** *incident, accident ou presque-accident ayant causé des dommages potentiels ou réels aux produits transportés ou au cours duquel des problèmes juridiques et/ou de (sécurité) alimentaire et sanitaire, de santé, de qualité et d'environnement* peuvent survenir ou surviennent.*		
⬇	**SLA**	**Responsable / Qui ?**	**Processus**
Informer la planification d'ECS	Jour 0	Transporteur Terminal ferroviaire Terminal maritime	Informer la planification d'ECS dès que l'incident/Accident survient ou dès que les contrôles de suivi révèlent une non-conformité considérée comme un incident.[1] *[1] joint brisé, dégâts, fuite unité d'alarme de température…*
⬇			
Informer les propriétaires internes	Jour 0	Planification d'ECS**	Informer le service client et les propriétaires concernés de prendre d'autres mesures.
⬇			
Définir des actions immédiates	Jour 0	Responsables(s)***	Le cas échéant des mesures immédiates sont prises par ses responsables.***
⬇			
Informer le client	Jour 0	Service client	Informer le client des premiers résultats des incidents et des mesures prises et, le cas échéant, attendre de nouvelles instructions du client. *Le cas échéant, le service juridique prendra contact avec le client pour traiter l'incident plus en détail.*
⬇			
Analyser l'incident	Jour 1	Responsables(s)***	Définir des mesures immédiates et, le cas échéant, prendre des mesures correctives et/ou préventives ou d'amélioration.
⬇			
Informer le gouvernement	Jour 1	Responsables(s)***	Le cas échéant, informer le gouvernement concerné de l'incident. Ex. FAVV, inspection environnementale, autres agences gouvernementals, …
⬇			
Donner un retour	Jour 5	Service client Responsables(s)***	Envoyer une résponse formelle au client avec le bilan de l'incident.
⬇			
Clore l'incident	-	Responsables(s)***	1) Suivi de l'incident et enregistrement complet dans le système ERP ; 2) Déterminer si l'efficacité des mesures doit être évaluée. Si la réponse et/ou la mesure est NOK, contacter le responsable ou la partie responsable pour obtenir des détails et/ou des mesures supplémentaires.
⬇			
Analyser et rapporter	Q	Coord. Q	Rapport trimestriel au ExCom concernant les incidents et l'efficacité des mesures correctives/préventives entreprises.
⬇			
STOP	* ** ***	ADR/IMDG, déversement, fuite, … Planification ECS : ferroviaire, routier, maritime, TCL, fret Responsable hiérarchique légal, responsable QESH, conseiller sécurité des marchandises dangereuses, équipe HACCP, …	

[1] Parties prenantes : clients, fournisseurs, autorités locales, responsables internes d'ECS, direction générale…
[2] Incident : un incident, accident ou presque-accident

Published version: 2.0

Procédure d'ECS en cas d'incident dans l'entrepôt :

Incident dans l'entrepôt	***Définition d'un incident :*** *incident, accident ou presque-accident ayant causé des dommages potentiels ou réels aux produits entrants, stockés ou quittant l'entrepôt, ou au cours duquel des problèmes juridiques et/ou de (sécurité) alimentaire et sanitaire, de santé, de qualité et d'environnement* peuvent survenir ou surviennent.*		
⬇	**SLA**	**Responsable / Qui ?**	**Processus**
Informer le responsable/chef d'equipe	Jour 0	Magasinier	Informer le responsable/chef d'équipe dès que l'incident/accident survient ou dès que les contrôles de suivi révèlent une non-conformité considérée comme un incident.[1] *[1] joint cassé, problème de température, dommages aux palettes/marchandises/matériels, produits illicetes, …*
⬇			
Définir des actions immédiates	Jour 0	Chef d'équipe/magasier	Le cas échéant, des mesures immédiates sont prises par le chef d'équipe/magasinier. p.ex. nettoyage, réparation, réempilage, zone Q, …
⬇			
Enregistrer l'incident et informer le SCI/la logistique	Jour 0	Chef d'équipe	Enregistrer l'incident dans l'outil d'entrepôt approprié (Apollo / Alerter / WH Tool / …).
⬇			
Informer le client/fournisseur	Jour 0	SCI Logistique	Informer le client/le fournisseur des premiers résultats des incidents et des mesures prises et, le cas échéant, attendre de nouvelles instructions du client/fournisseur.
⬇			
Analyser l'incident	Jour 1	SCI Logistique Responsables(s)***	Définir des mesures immédiates et, le cas échéant, prendre des mesures correctives et/ou préventives ou d'amélioration.
⬇			
Informer le gouvernement	Jour 1	Responsables(s)***	Le cas échéant, informer le fouvernement concerné de l'incident. Ex. FAVV, inspection environnementale, autres agences gouvernementals, …
⬇			
Donner un retour	Jour 5	SCI Logistique	Envoyer une résponse formelle au client/fournisseur avec le bilan de l'incident.
⬇			
Clore l'incident	-	SCI Logistique Responsables(s)***	1) Suivi de l'incident et enregistrement complet dans le système ERP ; 2) Déterminer si l'efficacité des mesures doit être évaluée. Si la réponse et/ou la mesure est NOK, contacter le responsable ou la partie responsable pour obtenir des détails et/ou des mesures supplémentaires.
⬇			
Analyser et rapporter	Q	Coord. Q	Réunion trimestrielle sur la qualité à propos les incidents et l'efficacité des mesures correctives/préventives entreprises.
⬇			
STOP	* déversement, fuite, inondation… ** Le cas échéant : Responsable hiérarchique légal, service des plaintes, responsable QESH, conseiller sécurité des marchandises dangereuses, équipe HACCP, …		

Published version: 2.0

Procédure d'incident ICT (sécurité de l'information)

Incident de sécurité de l'information	***Définition d'incident :*** *écart, ou écart imminent, par rapport au niveau de service convenu. Il existe une procédure spécifique en cas d'incident informatique ; Seules les étapes de haut niveau du processus sont mentionnées ici. Il existe un plan de réponse aux incidents distinct, aligné sur le programme d'urgence pour les entreprises, pour les incidents dont l'impact dépasse la procédure standard.*		
⬇	**SLA**	**Propriétaire / Qui ?**	**Processus**
Acceptation de l'incident	0	Tout collègue ICT	L'incident est reçu, enrichi de détails pertinents, hiérarchisé et lié aux dossiers connexes. Le rapporteur est informé du résultat, avec un retour d'information en cas de rejet.
⬇			
Catégorisation et correspondance	0	Service Desk (rôle)	L'incident est classé par type et par complexité, vérifié pour les correspondances avec les enregistrements existants et attribué au groupe de résolution approprié pour le traitement.
⬇			
Analyse	0	Spécialiste ICT	L'incident est analysé pour comprendre sa cause profonde, son impact potentiel et sa portée. Des mesures sont prises pour limiter les dommages, et une solution appropriée est sélectionnée pour la résolution.
⬇			
Préparation de la récupération	Jour 0	Spécialiste ICT	Des mesures de rétablissement sont planifiées, les préparatifs nécessaires sont effectués et l'approche de rétablissement proposée est mise à l'essai pour en assurer l'efficacité avant d'être mise en œuvre.
⬇			
Récupération	Jour 0	Spécialiste ICT	Les actions de récupération sont exécutées et vérifiées pour garantir le résultat souhaité. Le journaliste est ensuite invité à approuver le résultat, confirmant ainsi la résolution réussie.
⬇			
Fermeture	Jour 0	Spécialiste ICT	Les solutions de contournement temporaires sont supprimées, la base de connaissances est mise à jour et l'enregistrement de l'incident est finalisé. Le rapport est officiellement fermé, suivi d'une surveillance et d'un examen pour s'assurer qu'il est complet et amélioré.
⬇			
Rapports/ Analyse des causes profondes	Jour 1-6	Gestion des TIC	Pour les incidents ayant un impact substantiel, un examen post-incident est effectué afin d'analyser les tendances et les causes profondes. Des actions correctives et préventives sont définies pour renforcer la résilience future et réduire les récidives.
⬇			
STOP			