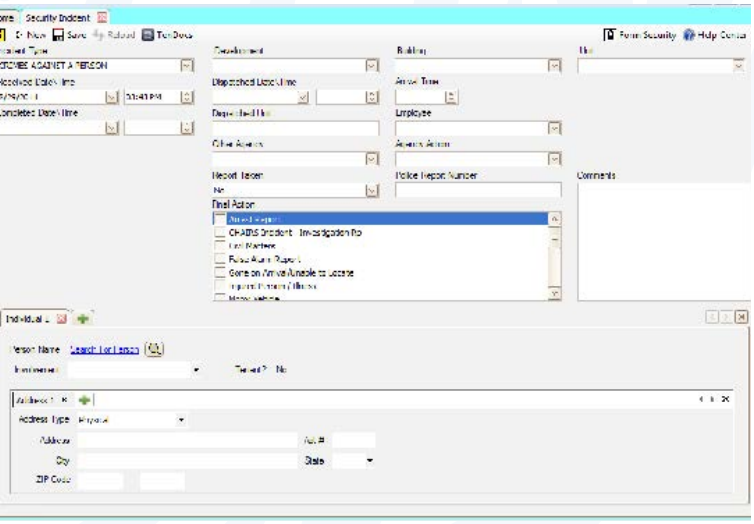
# CHAPITRE V

## Conformité aux politiques et procédures de sécurité



## Section B

## SYSTÈME D'ENREGISTREMENT DES INCIDENTS TOUCHANT À LA SÛRETÉ ET À LA SÉCURITÉ

**Date de promulgation:** 17 Avril 2015
**Revue technique:** 1er Mai 2017

## A. Introduction

1. La diversité et la multitude des contextes de menace dans lesquels le système de gestion du dispositif de sécurité des organismes des Nations Unies fonctionne exigent des mécanismes aidant à comprendre les menaces en question et mettant à la disposition des cadres supérieurs l'information requise pour les évaluer et les atténuer. La connaissance du type, du lieu et de l'impact des incidents qui ont, intentionnellement ou accidentellement, des effets néfastes pour le personnel, les programmes, les locaux et les actifs des Nations Unies sert de fondement à cette compréhension et guide les réactions appropriées.

2. Le système d'information sur les incidents touchant à la sûreté et à la sécurité est un outil destiné à recueillir de l'information sur les incidents qui touchent le système de gestion du dispositif de sécurité des organismes des Nations Unies afin de reconnaître les menaces et les incidents en vue de contribuer à une perception de la situation qui permet une réaction efficace, y compris les exigences relatives à l'atténuation et l'examen des modalités fonctionnelles conformément aux pratiques de gestion des risques de sécurité.

3. Le système d'information sur les incidents touchant à la sûreté et à la sécurité permet aux utilisateurs de faire ce qui suit :

   a) **Constater** : Reconnaître qu'un incident a eu lieu et le signaler à d'autres personnes;
   b) **Consigner** : Mettre des données en mémoire
   c) **Présenter une demande d'information pour appuyer l'analyse** : Mettre l'information en contexte pour que les responsables de la gestion de la sécurité la consultent et l'analysent;
   d) **Diffuser** : Diffuser les produits d'information.

## B. Objet

4. La présente politique a pour but de définir le type d'incident que le système d'information sur les incidents touchant à la sûreté et à la sécurité doit consigner en indiquant la taxonomie des incidents, en précisant les responsabilités concernant la consignation des incidents en question et en donnant des instructions sur les processus de consignation et d'acceptation.

## C. Application

5. La présente politique s'applique à l'ensemble du personnel employé par les organisations du système de gestion du dispositif de sécurité des organismes des Nations Unies qui exerce une fonction de sécurité dans le *Manuel des politiques de sécurité*, chapitre II, section A, « Cadre de référence sur les rôles et responsabilités dans le système de gestion du dispositif de sécurité des organismes des Nations Unies » du système de gestion de la sécurité des Nations Unies. Elle s'applique en particulier à l'ensemble des acteurs du système de gestion de la sécurité des Nations Unies auquel fait référence le « Cadre de référence des rôles et des responsabilités », y compris le personnel employé par les organisations du système de gestion du

dispositif de sécurité des organismes des Nations Unies qui a la responsabilité de « signaler tous les incidents de sécurité dans un délai opportun ».

6. La présente politique traite uniquement l'utilisation du système d'information sur les incidents touchant à la sûreté et à la sécurité. Elle ne modifie pas et ne définit pas les réactions aux incidents. Les instructions permanentes relatives aux réactions appropriées de gestion des incidents, de même que les politiques et les directives du système de gestion du dispositif de sécurité des organismes des Nations Unies et des organisations, énoncent les réactions appropriées aux incidents selon le cas..

## D. Responsabilités concernant le signalement des incidents de sécurité

7. Conformément au « Cadre de référence sur les rôles et les responsabilités », tout le personnel employé par les organisations du système des Nations Unies est tenu de « signaler tous les incidents de sécurité dans un délai opportun »[1].

8. De plus,aux termes du « Cadre de référence sur les rôles et les responsabilités » le responsable désigné doit, le cas échéant, tenir les membres de l'équipe de coordination du dispositif de sécurité et les dirigeants de chaque organisation dans le lieu d'affectation, au courant de toutes les informations et mesures relatives à la sécurité prises dans le pays.

## E. Utilisation du système d'information sur les incidents touchant à la sûreté et à la sécurité

### Exigences et restrictions

9. Le système d'information sur les incidents touchant à la sûreté et à la sécurité sert principalement à consigner les incidents qui ont eu des effets néfastes pour le personnel, les programmes, les activités, les locaux, les installations et les actifs des Nations Unies, ou les incidents qui pouvaient ou qui visaient à causer de tels effets.

10. Le signalement de tout incident qui met en cause ou qui touche le personnel, les programmes, les activités, les locaux, les installations et les actifs des Nations Unies est obligatoire.

11. On peut également recourir au système d'information sur les incidents touchant à la sûreté et à la sécurité pour consigner les incidents qui ne mettent pas en cause ou qui ne touchent pas les Nations Unies, et ce, à la discrétion de l'administrateur le plus expérimenté en matière de sécurité dans chaque pays. Cependant, les données relatives à des incidents qui ne touchent pas les Nations Unies et qui ont été signalées par le système d'information sur les incidents touchant à la sûreté et à la sécurité ne peuvent pas être utilisées à des fins officielles par des entités des Nations Unies. Ces données sont réservées au pays qui les soumet conformément à ses propres instructions permanentes. Comme ces données ne sont pas vérifiées ou acceptées

[1] Conformément au *Manuel des politiques de sécurité*, chap. II, sect. B : « Cadre de reference des roles et des responsabilités dans le système de gestion de la sécurité des Nations Unies », et à la section P, du système de gestion de la sécurité des Nations Unies, « le personnel employé par les organisations du système des Nations Unies [doit] signaler en temps utile tous les incidents de sécurité ».

conformément aux règles et aux normes établies dans la politique ou dans le manuel du système d'information sur les incidents touchant à la sûreté et à la sécurité, elles ne peuvent être utilisées qu'aux fins définies dans les instructions permanentes de chaque pays.

**Responsabilités concernant l'utilisation du système d'information sur les incidents touchant à la sûreté et à la sécurité**

12. L'administrateur le plus expérimenté en matière de sécurité est la personne chargée de conseiller le responsable désigné dans un secteur désigné et de consigner les incidents dans le système d'information sur les incidents touchant à la sûreté et à la sécurité. L'administrateur le plus expérimenté en matière de sécurité est normalement le conseiller en chef pour la sécurité ou le conseiller pour les questions de sécurité, le chef du service de sécurité, le coordonnateur des mesures de sécurité sur le terrain, le responsable des questions de sécurité de l'organisme ou le coordonnateur pour les questions de sécurité dans le pays, mais peut également être quelqu'un d'autre. L'administrateur le plus expérimenté en matière de sécurité peut seulement être un membre du personnel chargé des mesures de sécurité indiqué dans le« *Cadre de référence sur les rôles et les responsabilités* ».

13. La responsabilité de veiller à ce que les incidents soient signalés ne peut pas être déléguée, contrairement à la responsabilité de soumettre les données dans le système d'information sur les incidents touchant à la sûreté et à la sécurité qui peut faire l'objet d'une délégation. En consultation avec le responsable désigné et l'équipe de coordination du dispositif de sécurité, l'administrateur le plus expérimenté en matière de sécurité, selonle besoin, délègue aux personnes éligibles (une personne ayant un rôle dans le système de gestion du dispositif de sécurité des organismes des Nations Unies) la responsabilité de soumettre et d'accepter les données relatives aux incidents dans le système d'information sur les incidents touchant à la sûreté et à la sécurité.

14. La Division des opérations régionales du Département de la sûreté et de la sécurité assure la supervision de l'application et de l'utilisation quotidiennes du système d'information sur les incidents touchant à la sûreté et à la sécurité et examine l'entrée des données conformément à la présente politique.

15. Afin de s'assurer que tous les incidents sontconsignés de façon conforme, le système d'information sur les incidents touchant à la sûreté et à la sécurité envoie automatiquement à l'administrateur le plus expérimenté en matière de sécurité, au responsable désigné ou au coordonnateur, et à l'officier de la Division des opérations régionales, un courriel énumérant tous les incidents consignés dans le système au cours de la semaine précédente et leur demande de vérifier que les données relatives à leurs secteurs respectifs sont complètes.

## F. Processus de consignation des incidents

16. L'entrée d'un incident dans le système d'information sur les incidents touchant à la sûreté et à la sécurité s'effectue en deux étapes :

- **(a) Première étape : Entrer les données concernant l'incident** : Toutes les données pertinentes concernant un incident, y compris les personnes ou entités

touchées, le moment et le lieu de l'incident et sa description, sont soumises dans l'interface utilisateur du système d'information sur les incidents touchant à la sûreté et à la sécurité. Les données sont conservéessous forme de version préliminaire dans un serveur local jusqu'à ce qu'elles soient acceptées.

- **(b) Deuxième étape : Accepter les données concernant l'incident** : L'administrateur le plus expérimenté en matière de sécurité ou la personne désignée par celui-ci examine toutes les données concernant l'incident soumises dans le système d'information sur les incidents touchant à la sûreté et à la sécurité (première étape) pour déterminer si elles sont complètes et exactes. Après l'examen, l'administrateur accepte les données relatives à l'incident et soumises dans le système afin de les intégrer dans la base de données mondiale du système.

**Entrer les données concernant l'incident**

17. Conformément aux dispositions du paragraphe 7 ci-dessus, le personnel employé par les organisations du système des Nations Unies doit signaler les incidents au personnel du système de gestion du dispositif de sécurité des organismes des Nations Unies qui assure sa consignation dans le système d'information sur les incidents touchant à la sûreté et à la sécurité. Seules les personnes éligibles déléguées par l'administrateur le plus expérimenté en matière de sécurité en poste dans un pays sont autorisées à soumettre les données relatives à l'incident directement dans le système d'information sur les incidents touchant à la sûreté et à la sécurité.

a) Incidents mettant en cause une seule organisation

18. Conformément au paragraphe 13 ci-dessus, une organisation peut soumettre dans le système d'information sur les incidents touchant à la sûreté et à la sécurité des incidents mettant en cause ou touchant son personnel, ses programmes, ses activités, ses locaux, ses installations et ses actifs suite à l'autorisation de l'administrateur le plus expérimenté en matière de sécurité, en consultation avec le responsable désigné et l'équipe de coordination du dispositif de sécurité.

a) Incidents mettant en cause des organisations multiples

19. Les incidents peuvent êtres consignés par plusieurs organisations, mais ne peuvent être éxaminés et consolidés manuellement que par l'administrateur le plus expérimenté en matière de sécurité. Ce dernier peut également décider de les mentionner au sein du système. Il peut prendre cette décision au cas par cas, sur place, et en consultation avec le responsable désigné et l'équipe de coordination du dispositif de sécurité.

a) Autres exigences relatives à la consignation

20. Les incidents doivent être consignés dans le secteur où ils se produisent. Si l'administrateur le plus expérimenté en matière de sécurité ou un autre membre d'une organisation du système de gestion du dispositif de sécurité des organismes des Nations Unies est informé d'un incident qui a eu lieu à l'extérieur de son secteur, il doit communiquer les détails dudit incident à l'administrateur le plus expérimenté en matière de sécurité du secteur où l'incident a eu lieu.

21. Les incidents doivent être consignés dans un délai de sept jours à compter de la date à laquelle l'administrateur le plus expérimenté en matière de sécurité fut informé de l'incident en question. Si l'incident est porté à son attention après l'expiration de ce délai, il convient toujours de le consigner pour garantir que tous les incidents sont transmis dans le système d'information sur les incidents touchant à la sûreté et à la sécurité. Lorsque plusieurs incidents ont eu lieu dans le cadre d'un événement donné, chaque incident doit être consigné séparément et ensuite relié aux autres incidents dans le système d'information.

22. Si l'administrateur le plus expérimenté en matière de sécurité d'un pays décide d'utiliser le système d'information sur les incidents touchant à la sûreté et à la sécurité pour consigner des incidents qui ne touchent pas les Nations Unies, l'équipe de coordination du dispositif de sécurité doit adopter des instructions permanentes concernant les exigences relatives à la consignation et à l'acceptation. Une fois lesdites instructions adoptées, l'administrateur le plus expérimenté en matière de sécurité doit demander à la Section de l'information relative à la gestion des crises du Département de la sûreté et de la sécurité de lui donner le pouvoir d'ajouter des incidents qui ne touchent pas les Nations Unies.

**Accepter les données concernant l'incident**

23. L'administrateur le plus expérimenté en matière de sécurité est chargé de garantir la qualité des données consignées relatives à l'incident en acceptant le bilan de l'incident.

24. L'acceptation d'un incident est nécessaire pour sa soumission dans la base de données du système d'information sur les incidents touchant à la sûreté et à la sécurité. A défaut, les données ne sont pas transmises dans le système.

25. L'administrateur le plus expérimenté en matière de sécurité peut déléguer le pouvoir d'acceptation uniquementà un administrateur en matière de sécurité (un membre du système de gestion du dispositif de sécurité des organismes des Nations Unies qui accepte les responsabilités et les obligations relatives à la gestion de la sécurité conformément au « *Cadre de référence sur les rôles et les responsabilités* »).

26. En principe, les fonctions déléguées d'entrée et d'acceptation ne doivent pas être confiées à la même personne.

27. Le processus d'acceptation des incidents dont les données sont divergentes ou manquent de clarté sera confié, le cas échéant, au système de gestion du dispositif de sécurité des organismes des Nations Unies du secteur désigné. Toutefois, et conformément à la présente politique et aux directives en vigueur, l'administrateur le plus expérimenté en matière de sécurité est tenu, avant d'accepter un incident, de s'assurer de la clarté et de la précision des données.

**Réaction aux incidents**

28. Le système d'information sur les incidents touchant à la sûreté et à la sécurité est principalement un mécanisme de consignation. Il ne remplace pas les instructions

permanentes des organisations du système de gestion du dispositif de sécurité des organismes des Nations Unies concernant le signalement des incidents et n'entraîne pas de réaction à un incident. Dans plusieurs cas, un dossier pourrait être créé dans le système d'information sur les incidents touchant à la sûreté et à la sécurité si des mesures ont été prises en réaction à un incident.

29. Les organisations du système de gestion du dispositif de sécurité des organismes des Nations Unies doivent disposer de plans établis de gestion des incidents critiques et d'intervention conformément à leurs propres directives internes sur la gestion des incidents.

## G. Avertissement

30. L'information soumise dans le système d'information sur les incidents touchant à la sûreté et à la sécurité est confidentielle et soumise aux règles, règlements et procédures des Nations Unies concernant le traitement de l'information. Son utilisation est réservée aux entités du système de gestion du dispositif de sécurité des organismes des Nations Unies. Toute autre utilisation nécessite la permission du Département de la sûreté et de la sécurité.

## H. Dispositions finales

31. La présente politique est destinée à être distribuée à l'ensemble des organisations et du personnel du système de gestion du dispositif de sécurité des organismes des Nations Unies auxquels s'applique le *Manuel des politiques de sécurité*, chapitre III, (« Application du système de gestion du dispositif de sécurité des organismes des Nations Unies »).

32. La présente politique entre en vigueur le 17 avril 2015.

33. Les paragraphes 6.16 et 6.17 de la section E du chapitre VI du Manuel de sécurité des Nations Unies (2006) sont abrogés.