	National Defence Défense nationale		Retour à la liste des DED

DATA ITEM DESCRIPTION – DESCRIPTION DE DONNÉES

1. TITLE – TITRE	2. IDENTIFICATION NUMBER – NUMÉRO D'IDENTIFICATION
PLAN D'INTERVENTION EN CAS D'INCIDENT	**DED 3.10.10**

3. DESCRIPTION / PURPOSE – DESCRIPTION / OBJET

Le plan d'intervention en cas d'incident a pour objet de détailler les processus et les procédures de l'activité d'intervention en cas d'incident qui couvre la préparation au confinement, à l'éradication et au rétablissement, ainsi que les activités après incident. Les systèmes militaires doivent comporter des éléments pour le confinement, l'éradication, le rétablissement et l'analyse a posteriori appropriés en fonction de la criticité de la mission et de la menace sous-jacente liée à l'incident.
La phase de détection et d'analyse doit être couverte dans le plan de surveillance continue, LDEC 3.10.9, où les procédures et les outils de détection et d'analyse sont définis et mis en place.

4. APPROVAL DATE DATE D'APPROBATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE PREMIÈRE RESPONSABILITÉ (BPR)	6. GIDEP APPLICABLE APPLICABLE AU GIDEP
ÀD	Autorité technique (AT) de l'OSAN	S.O.

7. APPLICATION / INTERRELATIONSHIP – APPLICATION / INTERDÉPENDANCE

Consultez la LDEC 3.10.10 et le paragraphe 3.10.10 de l'EDT.
Cette DED énonce les instructions relatives au format et au contenu des données produites dans le contexte des tâches énoncées dans l'EDT pour le fonctionnement et l'entretien du Système d'alerte du Nord.

8. ORIGINATOR – AUTEUR	9. APPLICABLE FORMS – FORMULES PERTINENTES
AT OSAN	AUCUNE.

10. PREPARATION INSTRUCTIONS – INSTRUCTIONS SUR LA PRÉSENTATION DES DONNÉES

10.1 Document source

10.1.1 EDT de F et E du SAN section 3, paragraphe 3.10.10.
10.1.2 U.S. National Institute of Standards (NIST) SP 800-61 Rev. 2, Computer Security Incident Handling Guide (doi: SP800-61 Rev. 2).
10.1.3 Élaboration d'un plan d'intervention en cas d'incident de la technologie opérationnelle et de la technologie de l'information, Sécurité publique Canada, 2020, ISBN : 978-0-660-35443-9.

10.2 Contenu et format

10.2.1 Le plan d'intervention en cas d'incident doit être préparé et livré selon le format de l'entrepreneur.

10.2.2. L'Entrepreneur doit établir et mettre en œuvre un plan d'intervention en cas d'incident qui doit documenter ce qui suit :
- a. Prendre en considération :
  - i. Les pertes potentielles de fonction du système et leurs répercussions sur la mission, à partir du rapport de l'ACMEB.
  - ii. Les risques évalués, comme ceux décrits dans les rapports d'évaluation des risques.
  - iii. Les contraintes d'intervention (p. ex. technologie, ressources, temps, lois et règlements, etc.).
- b. Le plan doit comprendre les objectifs, les procédures, les outils à l'appui et les ressources nécessaires pour intervenir en cas d'incident.
- c. Le plan doit comprendre un plan de reprise après sinistre qui inclut des objectifs en matière de confinement, d'éradication et de rétablissement :

i. Les objectifs en matière de confinement liés aux répercussions des pertes de fonction du système doivent être définis.
ii. En ce qui concerne les menaces relevées durant l'évaluation des risques qui sont associées à un accès persistant, des objectifs en matière de confinement et d'éradication doivent être définis.
iii. Des objectifs en matière de rétablissement doivent être établis pour chaque perte de fonction du système, en tenant compte des missions du MDN/des FAC, de leurs opérations et des capacités que les fonctions du système appuient. Les objectifs doivent être définis en fonction des paramètres d'assurance de la mission (p. ex. laps de temps, pourcentages, etc.).

d. Cela inclut une procédure d'analyse a posteriori, dans laquelle :
i. Les répercussions de l'incident sont documentées.
ii. Les risques de renouvellement de l'incident sont relevés et gérés.
iii. Le rendement des procédures d'intervention en cas d'incident est mesuré par rapport aux objectifs définis à l'alinéa c).
iv. Des solutions pour améliorer les interventions en cas d'incident sont définies lorsque le rendement observé ne répond pas aux objectifs.

10.2.3. La catégorisation de sécurité du plan d'intervention livrable en cas d'incident doit être effectuée lors de la création du document, car le plan d'intervention en cas d'incident, ou certaines de ses parties, pourraient être protégés. L'étiquetage et le marquage de sécurité, ainsi que la manipulation, l'entreposage et la transmission du plan d'intervention en cas d'incident doivent être mis en œuvre conformément aux Ordonnances et directives de sécurité de la Défense nationale (ODSDN). Outre le marquage de sécurité, qui est placé dans l'en-tête et le pied de page de chaque page, un ensemble d'énoncés informatifs sera imprimé sur la couverture, ou la première page du document et, dans certains cas, également sur la page verso (au verso de la page de titre ou de la couverture) selon les besoins.

10.2.4. Il incombera à L'Entrepreneur de mener la gestion des changements, tel que décrit ci-dessous :

a. Le plan d'intervention en cas d'incident doit comprendre une section sommaire de l'historique des modifications, qui renferme ce qui suit :
i. Un identifiant clair et unique de la version/révision pour chaque soumission ou nouvelle soumission du plan d'intervention en cas d'incident.
ii. Une identification claire des révisions ou des modifications apportées au document par rapport à sa soumission précédente.
iii. Le bien-fondé des révisions et des modifications.

b. Toutes les révisions/modifications mentionnées ci-dessus doivent être clairement définies dans le document à l'aide de la fonction de suivi des modifications appropriée du logiciel de traitement de texte utilisé pour produire le document, par exemple, fonction de « Suivi des modifications » dans Microsoft-Word®, barres latérales, etc.

Page 2 de 2
Décembre 2020