	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 DES PRINCIPES DE BASE DE LA CYBER-SÉCURITÉ	**DED 3.10.8**

3. DESCRIPTION / PURPOSE – DESCRIPTION / OBJET

Le Plan des principes de base de la cybersécurité vise à démontrer comment L'Entrepreneur mettra en œuvre les quatre principales stratégies du Centre canadien de réponse aux incidents cybernétiques (CCRIC) pour atténuer les cyberintrusions ciblées.

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

Consulter la LDEC 3.10.8 et le paragraphe 3.10.8 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 3.10.8.
10.1.2 Les quatre plus importantes stratégies pour atténuer les cyberintrusions ciblées, CCRIC, mai 2019.

10.2 Contenu et format

10.2.1. Le Plan des principes de base de la cybersécurité doit être préparé et livré selon le format de L'Entrepreneur.

10.2.2. L'Entrepreneur doit établir et mettre en œuvre un plan écrit sur les principes de base de la cybersécurité pour l'OSAN qui doit documenter, au minimum, ce qui suit :

a. Un plan d'établissement d'une liste blanche des applications décrivant la façon dont le système interdira l'exécution de logiciels malveillants et de programmes non approuvés.
b. Une description du processus de gestion des correctifs pour garantir que les applications logicielles et systèmes d'exploitation du système demeurent exempts de vulnérabilités connues. Au minimum, les vulnérabilités connues sont celles qui sont répertoriées dans la base de données MITRE portant sur les vulnérabilités et expositions communes.
c. Un plan de gestion du cycle de vie du système d'exploitation décrivant la façon dont les systèmes d'exploitation :
   i. Demeureront pris en charge par les fabricants d'équipement d'origine (FEO) au chapitre des correctifs de sécurité en tout temps pendant le cycle de vie du système.
   ii. Demeureront évolutifs au fil des progrès des technologies de sécurité des systèmes d'exploitation.
d. Seront dotés d'un plan de restriction des privilèges administratifs intégré aux logiciels et aux systèmes d'exploitation en fonction des tâches de l'utilisateur.
e. Une liste des biens où les éléments a) à d) ne seront pas présents. Pour chaque élément :
   i. Expliquer pourquoi le contrôle de sécurité ne sera pas effectué.
   ii. Présenter un plan de gestion du risque résiduel.

10.2.3. La catégorisation de sécurité du plan des principes de base de la cybersécurité livrable doit être effectuée lors de la création du document, car le plan des principes de base de la cybersécurité ou certaines de ses parties pourraient être protégées et/ou classifiées. L'étiquetage et le marquage de sécurité, ainsi que la manipulation, l'entreposage et la transmission du plan des principes de base de la cybersécurité 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. Les sections du document qui sont classifiées peuvent indiquer le niveau de classification de chaque élément numéroté (c.-à-d. en-têtes, paragraphes) en plaçant (SC), (C), (S) ou (TS) avant le texte.

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

a. Le plan des principes de base de la cybersécurité 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 des principes de base de la cybersécurité.
   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