1. DÉFINITIONS

Actif cybernétique (AC) — Matériel électronique qui :

a) Comporte des ports de communication ;
b) Comporte des ports de programmation ;
c) Possède une capacité sans fil ;
d) Accepte les supports amovibles ;
e) Possède une interface personne-machine qui peut être utilisée pour affecter la disponibilité, l'intégrité ou la confidentialité ;
f) Est doté d'un microprocesseur ou d'un élément logique programmable qui peut être reprogrammé après la fabrication.

Actif essentiel pour la cybersécurité (AEC) — Actif essentiel pour la cybersécurité qui exécute ou touche :

a) Les fonctions importantes pour la sûreté nucléaire ;
b) Les fonctions de sécurité nucléaire ;
c) Les fonctions de préparation aux situations d'urgence ;
d) Les fonctions de sauvegarde ;
e) Les systèmes auxiliaires qui pourraient nuire aux éléments a) à d).

Équipement cybernétique — tout matériel informatique, logiciel, micrologiciel ou autre technologie informatique (autre qu'un actif cyberessentiel) qui est connecté à un réseau d'Énergie NB ou qui est utilisé pour accéder, créer, modifier, stocker, traiter ou transmettre les données d'Énergie NB dans le cadre de l'exécution des obligations de l'entrepreneur en vertu de la présente entente.

Services cybernétiques — toute application, infrastructure ou tout service connexe fourni par un entrepreneur relativement à : tout actif désigné par Énergie NB comme un actif cyberessentiel.

2. EXIGENCES EN MATIÈRE DE CYBERSÉCURITÉ

Entrepreneur :

2.1 Déclare et garantit à Énergie NB que : (i) l'entrepreneur a une politique écrite et exécutoire en matière de cybersécurité et a établi et maintient un programme de cybersécurité conçu et mis en œuvre pour prévenir et détecter les incidents cybernétiques susceptibles de nuire aux AEC d'Énergie NB et pour y répondre ; ii) le personnel de l'entrepreneur (qui, aux fins des présentes exigences, comprend tout membre du personnel de l'entrepreneur ayant accès aux AEC d'Énergie NB) a suivi une formation appropriée sur la cybersécurité ;

2.2 Doit immédiatement révoquer tout accès aux AEC d'Énergie NB pour le personnel de l'entrepreneur qui est licencié ou qui n'a plus besoin d'accéder aux AEC d'Énergie NB ;

2.3 Doit aviser Énergie NB après avoir découvert une atteinte à la sécurité, un incident ou une vulnérabilité qui touche ou met en cause les AEC d'Énergie NB. L'entrepreneur doit également fournir à Énergie NB une description de la brèche, de l'incident ou de la vulnérabilité, de son incidence potentielle sur la sécurité, de sa cause, d'un plan de redressement et des mesures d'atténuation ou de correction recommandées ;

2.4 Doit : i) veiller à ce que les AEC fournies ne contiennent pas de maliciels, de publiciels ou d'espiogiciels ; et ii) effectuer des correctifs et des essais sur tout matériel informatique, y compris par l'exécution de logiciels anti-maliciels et de balayages de vulnérabilités, afin de cerner et de corriger ou d'atténuer les faiblesses ou les vulnérabilités en matière de cybersécurité ;

2.5 Veiller à ce que les données des AEC d'Énergie NB détenues par le fournisseur soient adéquatement protégées ;

2.6 Si l'Entrepreneur est tenu par Énergie NB de se défaire des AEC d'Énergie NB, il doit s'assurer que (i) l'élimination est faite de façon sécuritaire et en temps opportun et (ii) que toutes les données connexes sont également supprimées de façon sécuritaire ;

2.7 Doit fournir de la documentation qui décrit son cycle de vie de développement des actifs cybernétiques, son programme de gestion des correctifs, ses processus de mise à jour et ses caractéristiques de cybersécurité ;

2.8 Doit fournir des mises à jour pour remédier à toute vulnérabilité en matière de sécurité du bien cybernétique, divulguer ses mécanismes pour fournir des mises à jour, s'assurer que ses contrôles permettront à Énergie NB de vérifier l'authenticité et l'intégrité des mises à jour ;

2.9 Doit utiliser les pratiques exemplaires en matière de cybersécurité dans le développement de tout bien cybernétique ;

2.10 Doit se conformer à toutes les politiques, normes et procédures de sécurité d'Énergie NB qui peuvent être fournies par Énergie NB à l'entrepreneur de temps à autre ;

2.11 Doit s'assurer que seul le personnel de l'entrepreneur autorisé par Énergie NB est autorisé à accéder aux AEC d'Énergie NB, à les traiter, à les stocker ou à les transférer ;

2.12 Veiller à ce que les AEC d'Énergie NB soient adéquatement protégées au moyen d'un chiffrement approprié au repos et en transit, et utiliser une protection physique et logique appropriée des frontières en cas de traitement, de stockage ou de transmission ;

2.13 Doit effectuer les essais appropriés de l'AEC et de ses composants essentiels afin de donner l'assurance que toutes les vulnérabilités connues sont identifiées et éliminées, et fournir les résultats de ces essais à Énergie NB ;

2.14 Doit identifier et désactiver tous les ports logiques et accessibles au réseau non utilisé et désactiver tous les ports/protocoles physiques et logiques inutiles dans le AEC ;

2.15 Veiller à ce que des politiques et des procédures de vérification et de responsabilisation efficaces soient en place pour assurer la cybersécurité.

Énergie NB se réserve le droit de faire une vérification auprès de l'entrepreneur dans tous les aspects de la cybersécurité, y compris les processus de développement, les procédures, les pratiques et les méthodologies.

3. DOCUMENTATION SUR LA CYBERSÉCURITÉ et AUTRES EXIGENCES

Entrepreneur :

3.1 Rédigera une lettre de conformité qui énumère individuellement chacun des éléments de cybersécurité énumérés en 2. et indiquera « Se conformer » ou « Ne pas se conformer » pour chaque élément. Un énoncé devrait préciser les éléments « Ne pas se conformer ».

3.2 Emballer l'AEC dans un emballage scellé et inviolable.