CONFIDENTIEL
(lorsque complété)

Secteur *nom*
Nom Direction
Nom Division

Évaluation des menaces et des risques

du

Nom de l'établissement
Lieux

Numéro de dossier

Sector Security Coordinator/
Coordinateur de la sécurité sectoriel

TABLE DES MATIÈRES…...……...1

TABLE DES FIGURES:

PARTIE 1 – FORMULAIRE DE SIGNATURE ET D'APPROBATION

Location de l'établissement:

_____
Nom de l'établissement

_____
Adresse

Préparez par:

_____
Nom

Coordinateur de la sécurité sectoriel
_____
Titre

_____
Signature

Approuvez par: **(**nom de l'officier supérieur de l'établissement)
_____
Nom

_____
Titre

_____
Signature

Date envoyée à la division de la Gestion de la sécurité, des urgences et du renseignement (DGSUR):

_____
Date

DOCS Open File #:

_____
File # (if applicable)

Partie 2 – Introduction

2.1 Sommaire

…

2.2 Historique

…

2.3 Topographie

…

2.4 Aperçu

La portée de cette EMR se concentre sur l'espace que RNCan procure au *(Nom division/branche*). Bien que cette EMR se concentre sur l'espace occupé par RNCan, il prend en compte, également la sécurité globale du bâtiment et des menaces extérieures pour le propriétaire et la présence de locataires, de ses capitaux, de personnel et d'activités. Cette EMR vise le secteur dans son ensemble, tout en fournissant un regard focalisé sur les espaces, le matériel, le personnel qui travail directement ou qui soutient les programmes du *(Nom division/branche*). Les éléments suivants ont été évalués au court de cette EMR:

- Le personnel employé sur place;
- Le personnel critique sur place;
- Information Protégée/Classifiée;
- Technologie de l'information, valeur et branchements; et
- Biens.

2.5 Restrictions et hypothèses

La conduite et le rapport écrit décrivant les résultats des activités associées à cette EMR ont pris en compte un certain nombre de limites et de présomptions afin de fournir une représentation exacte du niveau de sécurité associée aux actifs et activités du *(Nom division/branche*).

Cette EMR a évalué la posture de sécurité du *(Nom division/branche*) en la comparant directement aux modalités de la norme de base énumérée au sein de la Politique sur la sécurité du gouvernement et celle de RNCan.

Partie 3 – Vue d'ensemble de la situation actuelle de la sécurité au SST.

3.1 Identification et évaluation

L'information et les opérations de *(Nom division/branche*) **sont *(critiques ou non-critique)* pour Ressources Naturelles Canada et pour le Secteur *(nom du secteur)* et plus particulièrement pour le programme *(nom du programme)*. Conséquemment, sa protection et sa disponibilité sont impératives pour soutenir la capacité fondamentale des activités du secteur.**

Tout au long de cette EMR, l'évaluateur a noté un certain nombre de biens qui entrent dans le champ d'application de cette évaluation:

3.2 Personnel

Il y a un effectif complet de personnel (Approximativement 98 personnes), y compris le personnel de support et étudiants, qui travaillent au CIT-S. Tout le personnel employé sur le site bénéficie d'un environnement de travail considéré sain et sécuritaire supporté par un programme de formation à la sécurité matériel et à la santé et sécurité au travail.

3.3 Renseignement / Information sensibles

De l'information Protégée et Classifiée est traitée et sécurisée à l'intérieur des locaux du *(Nom division/branche*). Bien que la responsabilité primaire pour la protection du matériel sensible soit dirigée principalement vers les personnes qui possèdent lesdits documents (gardiens), et le personnel de soutien administratif qui gère et traite l'information du ministère, les superviseurs jouent quand même rôle crucial en rappelant à l'ordre ou en faisant appliquer les normes de sécurité. Le *(Nom division/branche*) possède actuellement un nombre insuffisant de classeurs de sécurité approuvés par la GRC pour suffire aux besoins d'entreposage du matériel sensible au *(Nom division/branche*).

La grande majorité des travaux et de la recherche menée au sein du *(Nom division/branche*) n'est pas d'une nature sensible, cependant due à son programme *(nom du programme)*, il devient de nature critique et doit être considéré comme telle. Donc sa protection adéquate est nécessaire pour éviter qu'une situation d'embarras ne puisse pas se développer. Nonobstant l'information précédente, les employés du *(Nom division/branche*) sont rendus responsables de la sauvegarde de l'information sensible qui leur est attribuée ou la protection des résultats de leur recherche suivant les principes du << Besoin d'accès et de savoir >>, et à cette fin, l'employeur leur fourni les classeurs de sécurité nécessaires ainsi que

l'information et la formation en sécurité requise pour qu'ils comprennent clairement leurs obligations et responsabilités envers la sécurité.

L'EMR a relevé que le *(Nom division/branche*) offre un nombre restreint de déchiqueteurs de documents pour ses employées. Cet appareil est approuvé par la GRC pour déchiqueter les documents jusqu'au niveau de protection B. De plus, ce déchiqueteur est situé dans la zone d'opération. Bien que le *(Nom division/branche*) offre à ses employés un service de destruction de documents gérés et contrôlés, les déchiqueteurs doivent être identifiés avec le plus haut niveau de Protection ou de Classification que l'appareil peut déchiqueter selon les spécifications et les recommandations émies par la GRC.

3.4 Objets de valeurs

Un nombre de type régulier et attrayant (ordinateur, matériel mobilier, équipement technologique, et autres) de biens se retrouve sur le site du *(Nom division/branche*). Les petites caisses et carte de crédit du ministère doivent être sécurisées en tout temps dans un classeur approuvé par la GRC. Par conséquent, la valeur totale peut être décrite comme *(bas, moyen, élevé)* tant en valeur qu'en attractivité.

3.5 Interdépendance des biens, du personnel et des procédés critiques

Il existe une relation d'interdépendance entre les biens, les employés et les procédés critiques d'une organisation. Cette interdépendance est nécessaire non seulement pour le succès de l'organisation, mais aussi pour la livraison des services et pour les opérations de recherches scientifiques.

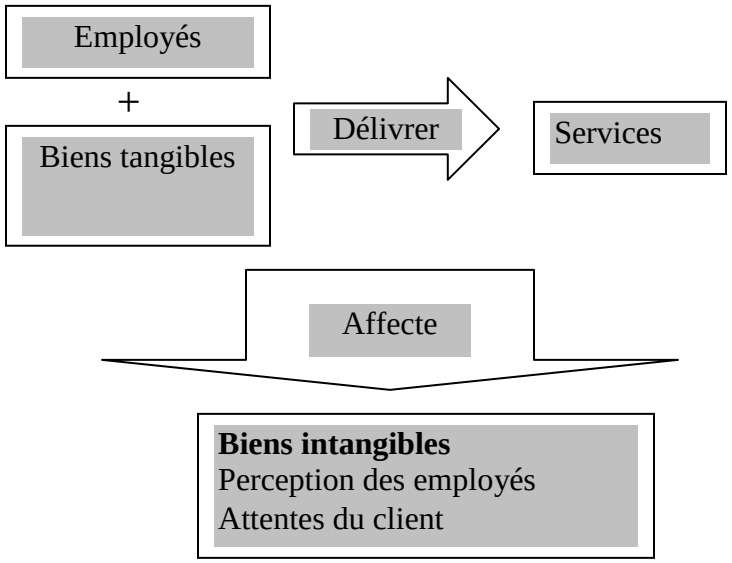

Figure 3 : Tableau des services d'interdépendance

Cette relation peut être décrite dans sa forme la plus simple par la formule (non-scientifique) suivante: les employés utilisant les biens (Tangible et Intangible), ou suivant un procédé critique, deviennent capables de livrer des services, de bâtir un produit ou de faire des opérations de recherches scientifiques. La perte d'un des éléments de base (biens, personnel ou procédés critiques) porte à une perte de capacité de production, engendrant ainsi une cessation ou en ralentissement important des activités de l'unité. Donc, il est impératif que l'employeur prenne des mesures raisonnables et adéquates pour protéger chacun des éléments identifiés ci-haut afin d'assurer la continuité de ses opérations.

Partie 4 – Évaluation des menaces et des risques

4.1 Détermination de la menace

Un certain nombre de menaces peuvent affecter un bien. Par exemple, dans le cas d'information sensible, les menaces pourraient comprendre : la modification, l'écoute, l'interruption, l'enlèvement, la destruction ou la divulgation non autorisée. Une EMR est donc menée pour identifier les menaces potentielles ainsi que les niveaux de risques associés. Cette EMR a identifié un certain nombre de menaces qui peuvent être résumées comme suit :

La violence en milieu de travail et les agressions, ci-après référées sous l'appellation assaut, est une menace toujours présente que l'employeur doit prendre en considération. La menace d'agression a été évaluée dans le cadre de cette EMR et est considérée comme allant de *(niveau)* en fonction du temps de la journée, l'emplacement et les activités menées par les employés.

Cette EMR a aussi considéré la menace dirigée vers les installations et les biens qu'elle protège; les trois menaces sont : l'introduction illicite (par effraction ou durant un manque de vigilance de la couverture des points d'accès), le vol et le vandalisme. Conformément aux indications de la méthodologie pour la conduite des EMR, le risque associé à l'introduction par effraction a été jugé *(Niveau)*, l'entrée de personnes sans passe de *(Niveau)*. Les risques associés au vol par une source intérieure (employés, entrepreneurs et les visiteurs) sont évalués de *(niveau)* alors que ceux attribuables aux agents extérieurs sont vus comme *(Niveau)* au *(Nom division/branche*).

La menace attribuable au vol ou retrait de matériel Protégé ou Classifié est considérée pour la menace interne comme (*Niveau*) et *(Niveau)* pour les agents externes. Cette évaluation est basée sur les facteurs tels que le matériel attrayant, sa valeur intrinsèque, son accessibilité et la faiblesse du contrôle d'accès à l'édifice. Le *(Nom division/branche*) a établi un programme de sécurité régional qui est supporté par le coordinateur de sécurité et par les politiques de sécurité de RNcan :

http://wwwint.nrcan.gc.ca/ci/ems/3/pdf/r-ssemd-po-dsm-e.pdf
http://wwwint.nrcan.gc.ca/ci/ems/3/pdf/r-ssemd-accfrm-e.pdf.

La disponibilité des technologies de l'information (TI) et de communication est considérée une valeur importante aux besoins opérationnels du *(Nom division/branche*). De

plus, la valeur de l'équipement de TI est évaluée à *(niveau)*. En ce qui concerne la menace d'interruption, et de refus de service, la connectivité informatique est offerte par le réseau de RNCan, qui est géré par les employés du ministère. La connectivité TI du *(Nom division/branche*) fait partie du réseau général qui est uniquement approuvé pour le traitement et stockage de matériel *Protégé A*. Il est possible de traiter et de communiquer le matériel *Protégé B* sur le réseau en utilisant le logiciel de chiffrement numérique <<Entrust>> qui élève le droit de sécurité de la station de travail au niveau *Protégé B*. Le risque d'interception associé à la transmission électronique des documents sensibles sur Internet est considéré comme *(Niveau)* à *(Niveau)* fondé sur la nature du réseau lui-même et l'attractivité de l'information disponible. Nonobstant ce qui précède, le traitement des documents sensibles, sans adopter des mesures de sécurité appropriées, en particulier celle qui est associée avec les documents secrets du ministère reste non conforme à la gestion des technologies de l'information (GSTI) et pose un risque d'embarras au ministère.

4.2 Détermination de la vulnérabilité

La principale vulnérabilité et faille que cette EMR a révélé, et qui devrait être une cause d'inquiétude pour *(Nom division/branche*), est (…) Le niveau actuel de la sécurité et la profondeur des mesures de contrôle d'accès associés à l'immeuble de base et par extension à *(Nom division/branche*), (*réponds ou ne répond pas)* aux normes de sécurité d'une *Zone d'Opération* selon le guide de la sécurité matérielle de la GRC. Bien que les programmes du *(Nom division/branche*) comptent beaucoup sur la vigilance de son personnel pour aider à la sécurité globale du plancher, le contrôle positif des clients et des visiteurs, ne doit pas être considérée comme une mesure d'atténuation conforme, mais plutôt comme un élément qui fait partie intégrante du continuum de la sécurité de l'installation. Sur la base des mesures de sécurité et de protection en place, la norme de sécurité du ministre ainsi que l'espérance de sécurité associée avec le personnel de RNCan, le risque de compromettre un renseignement protégé au *(Nom division/branche*) est considéré *(Niveau).*

4.3 Détermination du risque résiduel

Le tableau suivant est utile afin de déterminer le niveau du risque imputable au ministère en se basant sur la somme des menaces et des vulnérabilités. Une fois le risque calculé, celui-ci est divisé par la valeur des mesures de sécurité ou d'atténuation en place, ce qui permet de déterminer la valeur du risque résiduel selon les termes de la méthodologie approuvée par la GRC et RNCan.

Niveau de la vulnérabilité	Niveau de la menace				
	Très Faible	Faible	Moyen	Élevé	Très Élevé
Très Faible					
Faible					
Moyen					
Élevé					
Très Élevé					

Figure 4: Tableau des niveaux de la vulnérabilité et de la menace

L'espace occupé par le *(Nom division/branche*) est considéré comme une *Zone d'Opération*. Les procédures de sécurité établies associées au *(Nom division/branche*) avec les ressources technologiques et humaines des services de sécurité sont jugées non adéquates pour contrecarrer des tentatives d'entrée non-autorisées et répondre à la norme d'une *Zone d'Opération*. La posture de sécurité au *(Nom division/branche*) est déficiente, car il ne répond pas aux normes d'une zone de sécurité.

Les vulnérabilités principales soulevées par cette EMR sont la faiblesse et non-conformité du (…) Cette faiblesse peut être résolution par (…) La faiblesse de (…) du *(Nom division/branche*) pose un risque sur la sécurité de niveau *(Niveau).*

Partie 5 –Observations et recommandations

5.1 Sommaire des observations et recommandations

Tout au long de cette EMR, un nombre d'infractions et de défis de sécurité ont été relevés pour le *(nom du secteur)* et pour le *(Nom division/branche*), dont quelques-uns doivent être adressés dans les plus brefs délais. Nonobstant l'urgence attachée à quelques-unes des recommandations, le *(Nom division/branche*) est tout de même considéré comme un endroit sain et principalement sécuritaire. Les observations faites durant l'EMR sont énumérées ci-bas et accompagnées de recommandations qui aideront le *(Nom division/branche*) à corriger les défis ou à produire un plan d'action pour actionner lesdits défis.

1. **Observation 1:**

   Recommandation 1: Il est recommandé…

2. **Observation 2:**

   Recommandation 2 :

3. **Observation 3 :**

   Recommandation 3 :

4. **Observation 4 :**

   Recommandation 4:

5. **Observation 5 :**

   Recommandation 5 :

6. **Observation 6 :**

   Recommandation 6 :

7. **Observation 7 :**

   Recommandation 7 :

8. **Observation 8 :**

   Recommandation 8 :

9. **Observation 9 :**

   Recommandation 9 :

10. **Observation 10 :**

    Recommandation 10 :

Partie 6 - Conclusion

Le *(Nom division/branche*) est considéré comme non-conforme aux normes de la sécurité et à l'énoncé de la Politique sur la sécurité du gouvernement. Le (…) est le défi le plus important pour la gérance, suivi de près par (…).

Le niveau des menaces présent est évalué comme *(Niveau)* à *(Niveau),* créant ainsi un risque à la santé et sécurité des employés ainsi qu'un niveau de dommage *(Niveau)* à *(Niveau)* à la sécurité nationale. Les vulnérabilités non-conformités soulevées dans la partie des observations et recommandations de cette EMR indiquent clairement qu'il existe des risques ou au moins le potentiel de (…), causant ainsi non seulement un embarras au ministère, mais met aussi à risque les partenariats présent et futur.

Suivant la correction des lacunes mentionnées dans cet EMR, le *(Nom division/branche*) se verra accorder un statut de conformité avec les normes de sécurité du gouvernement. Toutefois, parce que la nature des menaces dirigées vers RNCan, ses biens et son personnel est toujours dans un état de flux constant, une réévaluation des menaces et de l'effectivité des mesures de protection est nécessaire. Cette réévaluation périodique doit être supportée par un programme de formation et sensibilisation à la sécurité, cela afin de s'assurer que le personnel et les biens du *(Nom division/branche*) sont protégés selon les plus vigoureux standards de protection.