ELECTRONIC DATA PROCESSING SECURITY

SÉCURITÉ EN MATIÈRE DE TRAITEMENT ÉLECTRONIQUE DES DONNÉES

POLICY OBJECTIVE

1. To ensure the protection of systems, data and services from accidental and deliberate threats to confidentiality, integrity, or availability thereof, thereby meeting the standards set by the Government of Canada.

OBJECTIF DE LA POLITIQUE

1. Veiller à la protection des systèmes, des données et des services contre toute menace, acciendentelle ou intentionnelle, en ce qui concerne le caractère confidentiel, l'exactitude et l'accessibilité des renseignements, de façon à satisfaire les normes établies par le gouvernement du Canada.

RESPONSIBILITIES

2. The National Headquarters unit responsible for electronic data processing security shall ensure:

   a. the development of security procedures relating to systems, data and services; and

   b. the monitoring and evaluation of electronic data processing systems and their surrounding environment in relation to the threat of compromise or unauthorized release of information.

3. The National Headquarters unit responsible for electronic data processing services shall ensure the implementation, coordination and supervision of the security policies, standards and procedures that affect electronic data processing within the Service.

4. Branch Heads, Deputy Commissioner, and any other persons who have electronic data processing systems under their control shall ensure that:

   a. data is compartmentalized for access purposes and authorized users are identified as required; and

RESPONSABILITÉS

2. L'unité responsable de la sécurité du traitement électronique des données à l'Administration centrale doit veiller:

   a. à la mise au point de procédures relatives à la sécurité des systèmes, des données et des services; et

   b. à la surveillance et à l'évaluation des systèmes de traitement électronique des données et de leur environnement au regard des situations qui pourraient compromettre la sécurité des renseignements ou conduire à leur divulgation non autorisée.

3. L'unité responsable des services de traitement électronique des données à l'Administration centrale doit veiller à la mise en oeuvre, à la coordination et au contrôle des politiques, des normes et des procédures relatives à la sécurité qui touchent le traitement électronique des données au sein du Service.

4. Les chefs de direction, les sous-commissaires, de même que toutes les personnes responsables de l'utilisation d'un système de traitement électronique des données doivent s'assurer:

   a. que les données sont cloisonnées aux fins d'accès et que les utilisateurs autorisés sont identifiés selon les besoins; et

b. an individual is identified to maintain a liaison with the National Headquarters unit responsible for electronic data processing security, to identify potential security concerns and ensure training of branch and regional personnel in electronic data processing security matters.

SECURITY CLASSIFICATION

5. The security classification or designation assigned to electronic data processing documentation, data, and programs shall be determined by the user in accordance with the procedures outlined for security of information.

ACCESS BY AUTHORIZED USERS

6. In order to gain access to the Service's electronic data processing systems, users shall require authentication codes or passwords. These codes and passwords shall be obtained in accordance with instructions issued by the unit responsible.

SEPARATION OF DUTIES

7. No one individual user shall perform all aspects of a critical process independently. For example, the user programming a modification shall not be responsible for updating the production library to incorporate that modification.

b. qu'une personne est nommée pour assurer la liaison avec l'unité responsable de la sécurité du traitement électronique des données à l'Administration centrale, une personne qui pourra identifier les difficultés éventuelles relatives à la sécurité et veiller à la formation du personnel de la direction et de la région en matière de sécurité du traitement électronique des données.

CLASSIFICATION DE SÉCURITÉ DES DONNÉES

5. C'est à l'utilisateur qu'incombe la responsabilité d'établir la classification ou la cote de sécurité attribuée aux documents, aux données et aux programmes, selon les procédures portant sur la protection des renseignements.

ACCÈS PAR DES UTILISATEURS AUTORISÉS

6. Afin d'avoir accès aux systèmes de traitement électronique des données du Service, les utilisateurs doivent obtenir des codes d'authentification ou des mots de passe, de la façon prescrite par l'unité responsable.

RÉPARTITION DES TACHES

7. L'ensemble des tâches reliées à un sytème important de traitement des données ne doit pas être confié à un seul utilisateur. Ainsi, la personne qui établit le programme apportant une modification quelconque ne doit pas être celle qui effectue la mise à jour connexe dans la programmathèque de production.

CONTRACTS

8. When developing electronic data processing contracts, all security concerns shall be weighed and appropriate clauses inserted in the contract to reflect these concerns. This shall be done in conjunction with the National Headquarters unit responsible for electronic data processing security.

MARCHÉS DE SERVICES

8. Lorsque l'on établit un marché de services portant sur le traitement électronique des données, il faut examiner attentivement toutes les questions reliées à la sécurité et inscrire dans l'entente des clauses tenant compte de ces préoccupations. L'unité responsable de la sécurité du traitement électronique des données à l'Administration centrale doit prendre part à cet examen.

ACCESS BY INMATES

9. Inmates shall be denied access to any electronic data processing systems or equipment:

   a. capable of retrieving information on either members of the Service or inmates;

   b. required to support the infrastructure of a particular institution; or

   c. capable of communicating with another terminal or computer outside the institution, except for those terminals on approved computer-assisted learning systems.

ACCÈS PAR DES DÉTENUS

9. Il est interdit aux détenus d'avoir accès à des systèmes ou à de l'équipement de traitement électonique des données:

   a. leur permettant d'obtenir des renseignements sur des membres du Service ou des détenus;

   b. assurant le soutien de l'infrastructure d'un établissement donné; ou

   c. leur permettant d'entrer en communication avec un terminal ou un ordinateur situé à l'extérieur de l'établissement, exception faite des terminaux branchés sur un système approuvé d'apprentissage assisté par ordinateur.

DISASTER PLANS

10. Plans shall be developed by those individuals responsible for data processing systems which provide for the re-establishment of the data processing service following a disaster. These plans shall identify essential services, data resources and minimum personnel resources required to maintain the service concerned. These plans shall be tested on an annual basis.

PLANS EN CAS DE DÉSASTRE

10. Les responsables des systèmes de traitement des données doivent préparer des plans prévoyant le rétablissement du service de traitement des données à la suite d'un désastre. Ces plans doivent comprendre une énumération des services essentiels et des sources de données, de même que préciser les ressources minimales nécessaires en matière de personnel pour assurer le fonctionnement du service. Il faut vérifier l'efficacité de ces plans une fois par année.

SECURITY INVESTIGATIONS

11. All suspected security violations and incidents occurring in the electronic data processing environment shall be investigated by the National Headquarters unit responsible for electronic data processing security. A written report shall be prepared on each incident.

AUDITS

12. The following audits shall be scheduled at a minimum:

    a. an audit to be carried out by the Royal Canadian Mounted Police Security Evaluation and Inspection Team, in accordance with the Treasury Board Administrative Policy Manual; and

    b. an annual audit of electronic data processing security operations conducted by the National Headquarters unit responsbible for electronic data processing security.

Commissioner,

ENQUÊTES DE SÉCURITÉ

11. L'unité responsable de la sécurité du traitement électronique des données à l'Administration centrale doit faire enquête chaque fois qu'une infraction ou un incident portant atteinte à la sécurité de l'environnement du système est soupçonné. Il faut rédiger un rapport sur chaque incident.

VÉRIFICATIONS

12. Il faut prévoir, tout au moins, les vérifications suivantes:

    a. une vérification effectuée par l'Équipe d'inspection et d'évaluation de la sécurité de la Gendarmerie royale du Canada, conformément au Manuel de la politique administrative du Conseil du Trésor; et

    b. une vérification annuelle de l'efficacité des mesures de sécurité s'appliquant au traitement électronique des données, menée par l'unité responsable de la sécurité du traitement électronique des données à l'Administration centrale.

Le Commissaire,

Rhéal J. LeBlanc