Dale - Security

Copy for Commerce

Department of Foreign Affairs and International Trade

CANADA

Ministère des Affaires étrangères et du Commerce international

UNCLASSIFIED

OTTAWA, April 18, 1995

CIRCULAR DOCUMENT

Admin. No. 4/95 (ISS)

Disciplinary sanctions for security breaches and violations

The security function is a responsibility shared by employees and management. All employees must recognize that misconduct or negligence on their part resulting in either a security breach or a security violation has serious consequences for the Department and themselves. Employees who have been subject to disciplinary sanctions for security matters will have this reflected in their annual appraisals.

2. The supervisor's responsibility in this regard must be understood. In the event of a security breach or violation, a management response is required. Supervisors must take responsibility for managing their resources, and this includes the administration of security policies and regulations in a fair, prompt and consistent manner. To aid in this process, supervisors and managers can call for advice and assistance from the Security Division (ISS). In serious cases, managerial recommendations and actions will be reviewed by the Disciplinary Committee.

3. The Department's policy is that employees who cause security breaches or who have repeated security violations are subject to the full range of administrative and disciplinary sanctions as set out in the departmental regulations and as required by the *Government Security Policy*. Any employee who receives five security infractions in any twelve-month period

FOR ACTION
Deputy Ministers
Assistant Deputy Ministers
Directors General
Directors
Heads of Mission

NON CLASSIFIÉ

OTTAWA, le 18 avril 1995

CIRCULAIRE ADMINISTRATIVE

N° 4/95 (ISS)

Mesures disciplinaires pour infractions et manquements à la sécurité

La fonction de sécurité relève tant des employés que de la direction. Chaque employé doit savoir qu'un écart de conduite ou une négligence de sa part entraînant une infraction ou manquement à la sécurité a de graves conséquences pour le Ministère et pour lui-même. L'employé visé par une sanction disciplinaire pour motif de sécurité aura une note à cet effet dans son évaluation annuelle.

2. La responsabilité du superviseur est sans équivoque. Il doit intervenir lorsqu'il y a infraction ou manquement à la sécurité. Les superviseurs assument la responsabilité de la gestion de leurs ressources, ce qui inclut l'administration des politiques et des règlements de sécurité de manière équitable, prompte et uniforme. Les superviseurs et les gestionnaires peuvent obtenir aide et conseils à cet égard auprès de la Direction de la sécurité (ISS). Dans les cas graves, les recommandations et les mesures prises par la direction seront examinées par le comité disciplinaire.

3. Selon la politique du Ministère, les employés coupables d'une infraction ou de manquements répétés à la sécurité sont soumis à la série complète des mesures administratives et disciplinaires décrites dans les règlements du Ministère et prévues par la *Politique du gouvernement sur la sécurité*. L'employé recevant plus de cinq avis de manquement à la

POUR SUITE À DONNER
Sous-ministres
Sous-ministres adjoints
Directeurs généraux
Directeurs
Chefs de mission

must be counselled in writing. Managers shall initiate disciplinary action in respect of any employee who causes a breach of security. Repeated offenses and more serious transgressions may lead to penalties such as suspension or discharge.

4. Definitions

(a) **Breach of security**: when any classified or designated information or assets have been the subject of unauthorized disclosure or unauthorized access. Without restricting its scope, a breach may include unauthorized disclosure by any person, theft, and loss or exposure in circumstances that make it probable that a breach has occurred. For example, there is a breach of security when a person:

— alters, keeps, destroys or removes classified or designated information or assets without authorization;

— accesses or operates departmental computers in violation of the departmental EDP security policy as set out in the Manual of Security Instructions.

(b) **Violation of security**: any act or omission that contravenes any provision of the security policy. For instance, there is a violation of security when a person:

— fails to designate or classify information according to departmental security policy;

— fails to lock up or otherwise physically protect classified or designated information or assets.

sécurité sur une période de douze mois doit recevoir des conseils par écrit. Les gestionnaires doivent imposer une mesure disciplinaire à tout employé ayant commis une infraction à la sécurité. Les manquements répétés ou les fautes plus graves peuvent entraîner des mesures comme la suspension ou le congédiement.

4. Définitions

a) **Infraction à la sécurité** : toute divulgation non autorisée d'un renseignement classifié ou désigné, ou tout accès à un bien classifié désigné, sans autorisation. L'infraction s'entend notamment, mais non exclusivement, d'une divulgation non autorisée, d'un vol ou d'une perte, ou d'un accès à des renseignement ou biens dans des circonstances qui ont l'apparence d'une infraction. Par exemple, une personne commet une infraction lorsqu'elle :

— modifie, conserve, détruit ou retire sans autorisation des renseignements ou des biens classifiés ou désignés;

— entre en communication avec les ordinateurs du Ministère d'une façon interdite par la politique sur la sécurité informatique du Ministère exposée dans le Manuel des instructions de sécurité.

b) **Manquement à la sécurité** : tout acte ou omission qui contrevient à une disposition de la politique sur la sécurité. Par exemple, une personne commet un manquement lorsqu'elle :

— omet de classifier ou de désigner des renseignements selon la politique de la sécurité du Ministère;

— néglige de mettre sous clé ou de protéger physiquement d'une autre manière l'information ou les biens classifiés ou désignés.

(c) **Need to know**: A fundamental principle of the security policy is to limit access to classified and designated information and assets to those whose duties require such access: that is for those who need to know the information or who need access to the assets. Application of the need-to-know principle restricts access within those levels to specific items, topics or types of sensitive information or assets.

5. This Circular Document is to be brought to the attention of all employees.

6. This Circular Document is cancelled effective April 1, 1996.

c) **Accès sélectif** : L'un des principes fondamentaux de la politique sur la sécurité est de limiter l'accès aux renseignements et aux biens classifiés ou désignés aux personnes dont les fonctions l'exigent, c'est-à-dire à celles qui doivent prendre connaissance des renseignements ou qui doivent avoir accès aux biens. L'application du principe de l'accès sélectif limite l'accès, à l'intérieur de ces niveaux, à certains articles, sujets ou types de renseignements ou de biens de nature délicate.

5. La présente circulaire doit être portée à l'attention de tous les employés.

6. La présente circulaire expire le 1er avril 1996.

Le sous-ministres des
Affaires étrangères,

Deputy Minister of
Foreign Affairs