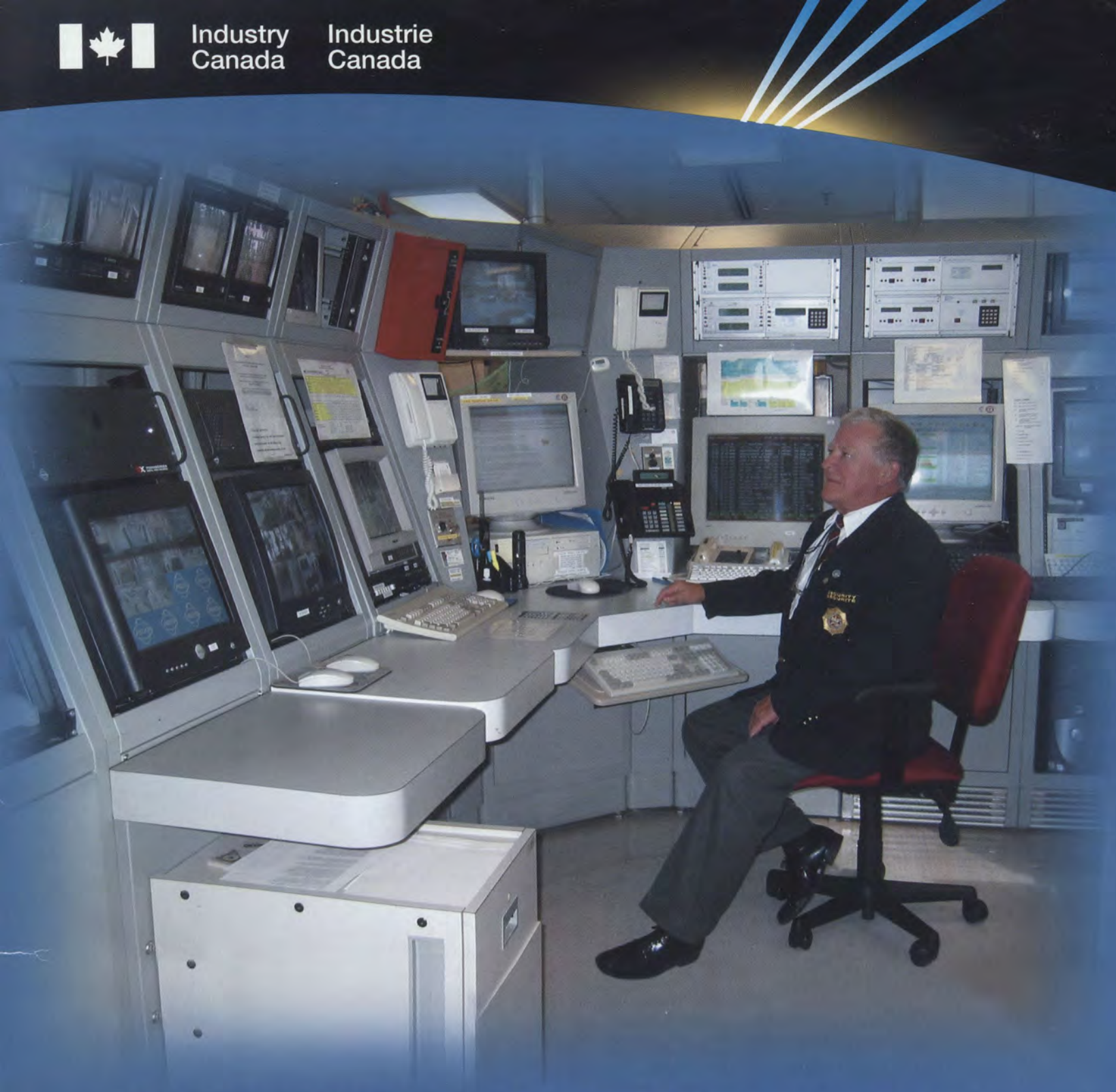
Industry Canada Industrie Canada



SECURITY SERVICES DIRECTORATE
DIRECTION DES SERVICES DE SÉCURITÉ

Canada

Security Services Directorate Website:
Site web de la Direction des services de sécurité :

http://icweb.ic.gc.ca/security-securite

IC Employee Information Line
1-866-599-4099
Ligne d'information pour les employé(e)s d'IC

Commissaire de la concurrence

Place du Portage I
50, rue Victoria
Gatineau (Québec)
K1A 0C9

Commissioner of
Competition

Place du Portage I
50 Victoria Street
Gatineau, Québec
K1A OC9

Télécopieur-Facsimile
(819) 953-5013

Téléphone-Telephone
(819) 997-3301

TO: Competition Bureau Staff

FROM: Sheridan Scott

DATE: September 17, 2004

SUBJECT: **The Handling and Disposal of Protected and Classified Records**

Introduction

This memorandum is further to my note of July 16, 2004 and sets out the Competition Bureau's ("Bureau") interim policies and procedures for the handling and disposal of records of a Protected or Classified nature. In conjunction with this memorandum, I would also ask all staff to read the Industry Canada pamphlet "A Guide to the Transmission, Storage and Destruction of Protected and Classified Information" found at the IC website:
http://icintra.ic.gc.ca/itsec-secti/engdoc/pol-pubs/docclass_e.pdf

A hard copy of the pamphlet is attached to this memorandum.

In conjunction with this, the Bureau Training Committee, in collaboration with Security Services Directorate of Industry Canada, is providing mandatory half day workshops on Security Awareness in the Workplace which will touch on a number of subjects discussed in this memorandum. These workshops will take place over the next few months.

It is important that all staff place the appropriate security classification on records. In this context, records are defined as in Section 2 of the *Competition Act* and include, among other things, correspondence, memoranda, paper documents, diskettes, disks, and machine readable records. With respect to investigative work conducted by the Bureau, protected records generally range from a categorization of Protected B to, on occasion, Protected C . In rare circumstances, Bureau records may be categorized as Classified records ranging from Confidential to Secret. Internally generated Human Resources records, which include personal information such as an individual's date of birth, home address, salary or SIN, are normally categorized as Protected A.

Accordingly, staff must mark all paper records, including note books, that they create in the course of business with the appropriate categorization. This requires some exercise of judgement. If staff have any doubt about an appropriate categorization, they should consult their supervisor. As for seized records, most of these records should be evaluated on an overall basis, and would most likely fall in the description of categories Protected B and, in rare circumstances, Protected C. Once records are categorized, they should be treated accordingly. With regard to electronic records, a further document, which provides guidelines for the handling of electronic records, will be forthcoming.

Removal of Protected and Classified Records from the Workplace

As emphasized in my e-mail message of July 16, 2004, at all times it remains everyone's responsibility to use the utmost care and caution when dealing with the security of confidential information regardless of type, medium or location.

As a result, prior to removal, all records categorized as Protected or Classified should be placed in a locked brief case with a Bureau business card securely attached. Once removed, such records should remain in the actual or constructive possession of staff in a manner similar to the process described in Bureau search procedures. Actual possession is the immediate and direct physical control over property. Constructive possession is having the conscious power and intention to exercise control over property, but without direct control of, or actual presence upon it. Constructive possession may occur when staff are on travel status and must leave records in their hotel room. In such a circumstance, records should remain locked in the brief case.

When records are in use they should remain in the actual control of staff and should only be worked upon or perused in as secure an area as possible. Staff should exercise care and caution when reading such records in public places such as airport lounges, restaurants, coffee shops or while in transit. When working at their residence, care and caution should also be exercised. In the event that the records are lost or misplaced, staff should promptly report such a matter to the ADC in their respective Division who will then report it to the Manager of Operations and Administrative Services.

Blue Box and Garbage Container

Material placed in the blue boxes is not shredded or disposed of in a secure manner and therefore blue boxes are not to be used for the disposal of Protected, Classified or any work related records. These records are to be shredded or placed in the shredding bins for future shredding.

Only newspapers, magazines, flyers or other like publications or documents in the public domain may be deposited in Blue Boxes or in garbage containers.

Staff should familiarize themselves with the locations of shredders and shredding bins on their floor. If any doubt exists about a document's disposal status, it should be shredded. Diskettes and disks of a Protected or Classified nature should be deposited with the Business Technology Centre, formally known as COMPASS, on the 16th floor of Phase I for disposal.

Cell Phones

Staff must ensure that messages are deleted on a regular basis and that passwords are in place. Lost or misplaced cell phones must be reported immediately to their ADC who will then report it to the Manager of Operations and Administrative Services. It is important to note that communication by cell phone is not completely secure and, as such, any information of a Protected or Classified nature is at risk of being intercepted. Therefore, caution and judgement must be used when using cell phones to communicate such information.

Blackberries

Due to the potentially sensitive nature of the data transmitted to Blackberries, all staff must ensure that a password is in place on this device. This ensures that any malicious attempts to break into the device causes it to erase all stored data. A lost or misplaced Blackberry must be reported immediately to their ADC who will report to the Manager of Operations and Administrative Services. The Competition Bureau's implementation of Blackberry service for employees at the Place du Portage complex ensures that all communication to and from the handheld unit are at a CSE approved level of encryption for Protected or Classified data and staff should feel comfortable using these devices.

Mailings

Inter-Office

String-tied messenger envelopes are not to be used for Protected or Classified records. The following procedure must be used.

Protected B and C records are to be double-enveloped. The outer wrapping shall not bear any marking which might indicate the security aspects of the contents. The inner wrapping shall be addressed and bear identification of the contents. If appropriate, other protective devices, such as seals, shall be applied. The inner wrapping must be marked as Protected B or Protected C and must also include a return address in the event that the envelope cannot be delivered, with an indication that the envelope is to be opened by the addressee only. (eg., The contents of this package are intended for _____ of _____. If wrongly received, do not open this package and please contact _____ at _____.) For Protected A and Classified records, please refer again to the pamphlet "A Guide to the Transmission, Storage and Destruction of Protected and Classified Information" found at the website:
http://icintra.ic.gc.ca/itsec-secti/engdoc/pol-pubs/docclass_e.pdf

E-Mails

While e-mails that are sent within the Bureau in Place du Portage go over a secure line, e-mails that are directed to regional offices or elsewhere in the Department or government are not secure. To remedy this security concern for records up to Protected B in nature, staff must use Public Key Infrastructure (PKI). PKI enables a user to encrypt an email and digitally sign it and send it securely. For more information on PKI, staff are directed to the Cintra website at http://cintra/Corporate/PublicKeyInfrastructure/ct00208e.asp for a detailed explanation. Any communication with the regions of material categorized as Protected A or B in nature must be sent using PKI capability. Protected C material cannot be sent by e-mail. If staff must send an e-mail by PKI, they should contact Donna Dale, the Bureau's Local Registration Authority, at 953-5179 for registration procedures.

Faxes

When sending Protected or Classified records by fax, it is also critical to ensure the highest level of protection from outside sources. The CERTIFAX encryption device must be used when faxing sensitive information between Bureau offices; that is between NCR and the Regions or between offices in the Regions. CERTIFAX secures sensitive fax transmissions from misdirection, inadvertent disclosure and attempted interception, ensuring sensitive fax transmissions remain

confidential. It does this by authenticating the fax's sender and recipient, and then encrypting the data for secure transmission. Please be sure to always use CERTIFAX when sending sensitive documents in this manner.

CERTIFAX machines are located on the 15th, 17th and 22nd floors and one will shortly be located on the 20th floor.

Unauthorized Access to Bureau Space

When unknown persons are sighted on any of the Bureau's floors, staff should challenge them and inquire as to the nature of their business and escort them to the appropriate person or location or escort them off the floor.

Staff should be aware that modifications have been made to the handicapped accessibility door mechanism to limit the potential for unauthorised entry. In order to activate the mechanism, staff must now swipe their card and press the button. Staff choosing to use this function to enter or exit must wait until the door has closed before proceeding to prevent any potential for unauthorised entry.

Clean Desk

Bureau policy is that at the end of the work day, staff must ensure that all Protected or Classified records are removed from their desks and elsewhere in their office and locked in a filing cabinet. With regard to closed offices, unless they are enclosed with wire mesh, the clean desk policy will apply. Should operational requirements mean that this policy cannot be followed fully, staff should discuss this matter with their ADC. Deputy Commissioners will advise their staff of any acceptable deviation from this policy within their respective Branches.

If staff are leaving and not returning to their office for the rest of the day or are away from their office for a day or longer, they must place the standard "Absent" sign on their desk top which indicates with whom to leave all records and mail (most likely the Division secretary). If that person is not at his or her desk, do not leave the records and either locate an alternate person or keep the records until the person returns. "Absent" signs were distributed recently but if for some reason you did not receive one, please contact Donna Dale, Operations Coordinator, at 953-5179 to receive one or you can go to her office which is located on the 23rd floor of Phase I.

Prior to leaving for the day, staff must check the printer to ensure that none of their Protected or Classified documents remain at the machine. The fax machine should also be checked to ensure that all incoming faxes are removed.

Conclusion

It is imperative that the policies and procedures outlined in this document be followed. The proper control of records is essential to the integrity of the Bureau as an efficient and respected law enforcement agency. As mentioned in my message of July 16, 2004, confidentiality is a core value of the Bureau. As a result, it is important that all persons who deal with the Bureau have assurance that all confidential information provided to the Bureau will be treated as sensitive and be subject to stringent security. Once more, I would like to stress that at all times it remains the responsibility of all staff when dealing with Protected or Classified records to use the utmost care and caution regardless of the work location. Failure to comply with the policies and procedures outlined in this memorandum may result in disciplinary measures.

Sheridan Scott

Att.

Examples of Protected Documents specific to the Competition Bureau

Section 29 of the Competition Act - Confidentiality

Protected B Documents

- Memoranda:
  - prepared of telephone calls and in person interviews;
  - prepared from information provided by complainants or industry people such as suppliers, customers, competitors;
  - to supervisors on cases;
  - recommending start of formal inquiry;
  - recommending use of formal powers.

- Any financial information that companies may provide, business plans, marketing plans, financial statements, contracts they have with other companies

- Summaries of Evidence

- Case Assessment memoranda

- Section 11 transcripts and returns of information, section 11 orders

- Warrants and Information until made public

- Any information that is received by other government departments in confidence

- Any information provided by foreign agencies with regard to joint investigations under MLAT

Protected C Documents

- Certain documents obtained in the course of merger examinations which could cause significant financial loss to a company if the information were to become public

Exemples de documents protégés spécifiques au Bureau de la concurrence

Article 29 de la Loi sur la concurrence - Confidentialité

Documents Protégé B

- Notes de service :
  - préparées à partir d'entrevues téléphoniques ou personnelles;
  - préparées à partir d'informations fournies par des plaignants ou des gens de l'industrie telle que des fournisseurs, des clients, des compétiteurs;
  - aux surveillants concernant des dossiers;
  - recommandant le début de l'enquête formelle;
  - recommandant l'utilisation des pouvoirs formels.

- Toute information financière que les compagnies peuvent fournir, des plans d'activités, des plans de commercialisation, des états financiers, des contrats qu'ils ont avec d'autres compagnies

- Sommaires de la preuve

- Note d'évaluation de dossier

- Transcriptions et états de renseignements de l'Article 11, ordonnances en vertu de l'Aticle 11

- Mandats et renseignements jusqu'à ce qu'ils soient rendus publics

- Tout autre renseignement reçu à titre confidentiel d'autres ministères du gouvernement

- Tout renseignement fourni par des organismes étrangers concernant des enquêtes mixtes selon le TEJ.

Documents Protégé C

- Certains documents obtenus dans le cadre d'examens de fusions qui pourraient causer d'importantes pertes financières à une compagnie si l'information devait devenir publique.

Security Screening Requirement Questionnaire

This questionnaire assists managers in determining the security screening requirements for employees and contractors.

For further information and clarification, contact Paul Pinaud, Manager, Personnel Security and Intelligence at (613) 954-4293.

Part 1.

Does the position require access to ***classified information/assets***, the compromise of which could reasonably be expected to cause injury to the ***national interest*** in one of the following areas:

a) **Economic Interest of Canada**

❑ **YES** ❑ **NO**

Includes valuable trade secrets and sensitive financial, commercial, scientific or high technology information that belong to the federal government including nuclear, biological or chemical weaponry, chemical technology and biotechnology; sensitive information relating to the legal tender of Canada, contemplated sale or purchase of securities or currency, contemplated changes in tariff rates, taxes, duties or any other revenue source and contemplated changes in the conditions of operation of financial institutions.

b) **International Affairs and Defence**

❑ **YES** ❑ **NO**

Includes diplomatic plans, negotiations and correspondence; analyses of domestic affairs of another nation; tactical and strategic defence plans and equipment; intelligence relating to subversive/hostile activities; sensitive information relating to communications or cryptographic systems.

c) **Cabinet Documents**

❑ **YES** ❑ **NO**

Includes memoranda, records of decisions, briefing notes, agendas, reports, minutes and draft orders.

Questionnaire relatif aux exigences en matière de sécurité

Le présent questionnaire aide les gestionnaires à déterminer quelles sont les exigences en matière de sécurité imposées aux employés et aux entrepreneurs.

Pour plus d'information ou pour obtenir des éclaircissements, veuillez communiquer avec Paul Pinaud, gestionnaire, Sécurité du personnel et du renseignement, au (613) 954-4293.

Première partie

La personne occupant le poste doit-elle avoir accès à de l'***information ou à des biens classifiés***, dont la compromission est susceptible de porter atteinte à l'***intérêt national*** dans l'un des domaines suivants :

a) **Intérêt économique du Canada**

❑ **OUI** ❑ **NON**

Secrets commerciaux importants et information financière, commerciale, scientifique ou liée à la haute technologie, de nature délicate, qui appartient au gouvernement fédéral, notamment dans le domaine des armes nucléaires, biologiques ou chimiques, de la technologie chimique et de la biotechnologie; information de nature délicate relative à la monnaie légale du Canada, à la vente ou à l'achat envisagés de sûretés ou de devises, à des changements envisagés des taux tarifaires, des taxes, droits, ou de toute autre source de revenus, et à des changements envisagés dans le fonctionnement des établissements financiers.

b) **Affaires étrangères et défense**

❑ **OUI** ❑ **NON**

Projets, négociations et correspondance diplomatiques; analyses des affaires intérieures d'un autre pays; plans et équipement militaires tactiques et stratégiques; renseignements reliés à des activités subversives/hostiles; information de nature délicate reliée aux systèmes de communications ou de chiffrement.

c) **Documents du Cabinet**

❑ **OUI** ❑ **NON**

Notes de service, rapports de décision, notes d'information, ordres du jour, rapports, comptes rendus et projets de décrets.

d) **Federal-Provincial Affairs**

❑ **YES** ❑ **NO**

Includes sensitive information relating to federal-provincial consultations or deliberations, constitutional negotiations and strategy and tactics adopted for the conduct of federal-provincial affairs.

If the position requires access to ***classified information/assets***, a ***security clearance*** is required. To determine the level of the *security clearance,* go to **"Part 2."** If **NOT**, go to **"Part 3."**

Part 2.

a) If the individual requires access to *classified information* marked **CONFIDENTIAL** and it's compromise could reasonably be expected to cause *injury* to the national interest, a ***security clearance*** at the ***Confidential*** level is required.

b) If the individual requires access to *classified information* marked **SECRET** and it's compromise could reasonably be expected to cause *serious injury* to the national interest, a ***security clearance*** at the ***Secret*** level is required.

c) If the individual requires access to *classified information* marked **TOP SECRET** and it's compromise could reasonably be expected to cause *exceptionally grave injury* to the national interest, a ***security clearance*** at the ***Top Secret*** level is required.

Part 3.

A ***Reliability Check*** is mandatory for every individual who does not require access to classified information or assets. (Please note that the terms *Basic Reliability* and *Enhanced Reliability* have been removed from the Treasury Board of Canada Secretariat effective February 1, 2002.)

(Revised 2003/01/27)

d) **Affaires fédérales-provinciales**

❑ **OUI** ❑ **NON**

Information de nature délicate reliée aux consultations ou délibérations fédérales-provinciales, aux négociations constitutionnelles ainsi qu'aux stratégies et tactiques adoptées pour les affaires fédérales-provinciales.

Si la personne occupant le poste doit avoir accès à de l'***information ou à des biens classifiés***, une ***autorisation de sécurité*** est requise. Pour déterminer le niveau de l'*autorisation de sécurité,* passez à la « **Deuxième partie** ». **SINON**, allez directement à la « **Troisième partie** ».

Deuxième partie

a) Si la personne doit avoir accès à de l'*information classifiée* portant la mention **CONFIDENTIEL** et dont la compromission est susceptible de porter *atteinte* à l'intérêt national, une ***autorisation de sécurité*** de niveau ***confidentiel*** est nécessaire.

b) Si la personne doit avoir accès à de l'*information classifiée* portant la mention **SECRET** et dont la compromission est susceptible de porter une *atteinte sérieuse* à l'intérêt national, une ***autorisation de sécurité*** de niveau ***secret*** est nécessaire.

c) Si la personne doit avoir accès à de l'*information classifiée* portant la mention **TRÈS SECRET** et dont la compromission est susceptible de porter *gravement atteinte* à l'intérêt national, une ***autorisation de sécurité*** de niveau ***très secret*** est nécessaire.

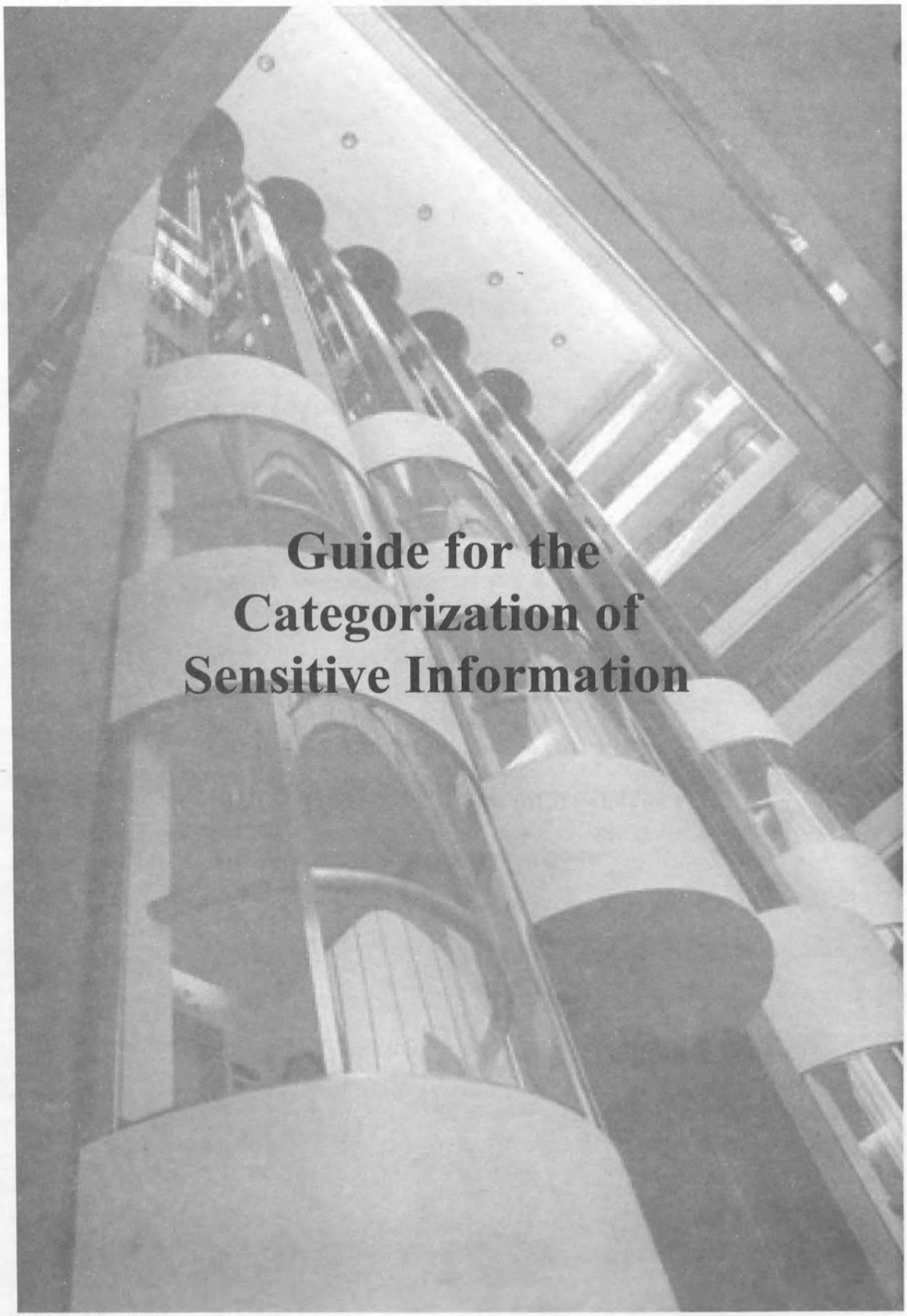
Troisième partie

Une ***Vérification de la fiabilité*** est requise pour toute personne n'ayant pas besoin d'accès à de l'information ou des biens classifiés. (Veuillez noter que les termes *Vérification de base* et *Vérification approfondie* ont été supprimés de la politique en matière de sécurité du Secrétariat du Conseil du trésor du Canada à partir du 1 février 2002.)

(Révisé 2003/01/27)

Industry Canada Industrie Canada

Canada



Guide for the Categorization of Sensitive Information

Date modified: 2004 - August

For information please contact:

Sandy Little
Manager
Security Training and Awareness and Regional Coordination
Security Services Directorate
Financial, Systems, Facilities and Security Branch
Comptrollership and Administration Sector

C.D. Howe Building
Room 327A - East Tower
235 Queen Street
Ottawa - K1A 0H5

Tel: (613) 954-4358 ❖ Fax: (613) 941-2380

E-Mail: little.sandy@ic.gc.ca

TABLE OF CONTENTS

Categorization of Sensitive Information

Categorizing sensitive information identifies the level of sensitivity of departmental information. It is the responsibility of the originator to determine the level of sensitivity. There are two separate levels of sensitivity: Protected Information and Classified Information.

Difference Between "Classified" and "Protected" Information

The classification of information refers to a determination that the sensitive character of the information is such that its unauthorized disclosure, modification or destruction could affect the national security or the national interest. By "national security" and "national interest", we mean that the unauthorized disclosure, modification or destruction of the information will possibly harm the political, social or economical stability of Canada. The marking of classified records as "Confidential", "Secret" or "Top Secret" facilitates their identification and ensures that they are treated in a manner that is consistent with their relative level of sensitivity. Examples of classified information include:

- Cabinet confidences (Confidences of the Queen's Privy Council for Cabinet) including Treasury Board Submissions;
- Information that relates to military and anti-terrorism intelligence operations;
- Strategic information that relates to international trade negotiations and other international events and activities which could affect the interests of Canada or its allies;
- Information that could pose a threat to the integrity of the democratic institutions of Canada;
- Information that could affect the ability of the Government of Canada to manage the economy of the country (macro-economic decisions); and
- Solicitor-client privileged information that relates to national security or national interest issues.

Because of the nature of its business, only a small portion of the information that is under the control of Industry Canada is classified.

Categorizing information as "Protected" refers to the determination that information that does not relate to the national security or the national interest is nevertheless sensitive and deserves protection. Records that contain protected information must be marked as "Protected A", "Protected B" or "Protected "C", depending on their relative level of sensitivity. Although some of the following categories of information may at times be "classified" as a result of extraordinary circumstances, they are generally considered as "protected":

- Trade secrets and commercial, financial, technical and scientific information of third parties;
- Personal information about an identifiable individual, including the home address and telephone number of the individual, personal identifiers such as the individual's social insurance number and, performance evaluative material, medical information and criminal records;
- Information obtained in confidence from provincial and municipal governments;

- Law enforcement records and investigations files;
- Information pertaining to the negotiation of grants and technical assistance to businesses;
- Plans for the management of personnel;
- Accounts of consultations and deliberations involving officers and employees of the department and/or staff of the minister;
- Communications plans on departmental business; and
- Solicitor-client privileged information that does not relate to national security or national interest issues.

Special Procedures for Handling Cabinet Documents

The Canadian government is based on a Cabinet system. Thus, responsibility rests not with a single minister but on a committee of ministers sitting in Cabinet. Cabinet ministers are collectively responsible for all actions of the Cabinet and they must support all decisions of the Cabinet whether directly involved or not and whether they agreed initially or not. However, to reach that final decision, all ministers must be able to express their views freely during the discussions leading up to Cabinet decisions. To allow this exchange of views to be disclosed publicly would result in the erosion of collective responsibility for ministers. As a result, the collective decision-making process has traditionally been protected by the rule of confidentiality which protects the principle of the collective responsibility while enabling ministers to engage in full and frank discussions necessary for the effective functioning of a Cabinet system of governmer

In order to preserve the essential character of confidentiality of Cabinet deliberations, subsection 69(1) of the Access to Information Act and subsection 70(1) of the Privacy Act provide that *Confidences of the Queen's Privy Council for Canada,* commonly called *Cabinet records*, are excluded from the application of these Acts. This means that Cabinet records do not have to be disclosed in response to an access request under the ATIP Acts. The authority to determine whether a specific record is a Cabinet record or not for the purposes of the ATIP Acts ultimately rests with the Privy Council Office (PCO), and a consultation procedure has been established to allow ATIP office in federal government departments to confirm the status of records as Cabinet records from PCO when processing ATIP requests. Having said that, it is important to note that at Industry Canada, the ATIP office is responsible for making the first determination that a document may contain Cabinet information and to initiate the consultation process with PCO. **As a result, all Cabinet records that are requested under the ATIP Acts must be sent to the ATIP ofice for review.**

The Government Security Policy (GSP) provides that records that contain information that is subject to subsection 69 (1) of the Access to Information Act and subsection 70(1) of the Privacy Act must be classified in the national interest, and they must at a minimum be marked as "Secret".

Categorization of Information that is Neither Classified or Protected

The following categories of information are not generally classified or protected:

- Information that is published or available for purchase by the public;
- Information that is posted on the departmental internet web site;
- Information that is kept in the departmental public registries;
- Information that has been disclosed under the Access to Information Act by the appropriate authority within the department;
- Departmental policies and procedures that are used by employees to perform their duties;
- Departmental budgetary information; and
- Grant and contracting information, with the exception of the proprietary information that is contained in the contract records.

It should also be noted that the GSP stipulates that the classification and protection of information must not be used to illegally protect information that relates to fraudulent and other malicious acts.

Disclosure of Sensitive Information Under the Access to Information Act or the Privacy Act

In accordance with the principle that Acts of Parliament take precedence over policies and procedures, decisions to refuse access to information that has been requested under the ATIP Acts are governed only by the exemption and the exclusion provisions of those two Acts. As a result, the security level of a record is not a factor in that decision. Having said that, information to be disclosed under the ATIP Acts must first be declassified or downgraded before it is released, so that it is no longer subject to the security measures established under the GSP, and the originator of the document must be involved in that process. The declassification and downgrading process is further explained later in this guide.

Steps in Categorizing Records for Security Purposes

The process of categorizing and marking records is divided into the following steps:

Step one:

Does the information relate to the national interest or to the national security of Canada?

Step two:

If so, then would the permanent or temporary loss of confidentiality, integrity or availability of the information cause an injury as defined in the exemption or exclusion provisions of the Access to Information Act or the Privacy Act?

Step three:

Assessing the gravity of the injury to the national interest or the national security

- For an injury, the record shall be marked **"Confidential"**;
- For a serious injury, the record shall be marked **"Secret"**;
- For an exceptionally grave injury, the record shall be marked **"Top Secret"**.

Step four:

If the information does not relate to the national interest or to national security, would the permanent or temporary loss of confidentiality, integrity or availability cause another type of injury as defined in the exemption or exclusion provisions of the Access to Information Act or the Privacy Act?

Step five:

If yes, determine if the compromise were to cause:

- An injury, then the record shall be marked **"Protected A"**;
- A serious injury, then the record shall be marked **"Protected B"**;
- An extremely grave injury, then the record shall be marked **"Protected C".**

Marking the Records for Security Purposes

The requirements for the security marking of records are as follows:

a. ***The marking must reflect the level of the most sensitive information that is contained in the document:***
This means that the security marking must be at the level of the most sensitive information that is contained in the document so as to ensure that the highly sensitive information is adequately protected. For example, a record containing "secret" and "protected B" information shall be marked as "secret" and be protected as if it contained all "secret" information in order to ensure that the "secret" information is adequately protected.

b. ***The marking must be in eye-readable form:***
The marking must be easily visible so that managers and employees can identify a sensitive record just by physically looking at it. Although this requirement could possibly make a record more vulnerable if it is left unattended in a public place, the visibility of the marking is meant to prompt managers and employees to be more vigilant in the manipulation of such records.

c. ***The marking must be applied on a specific location on the document and the circulation of the document is subject to certain rules.***

Protected Records Marking

- "Protected" in upper right corner of the face of the document;

- Reason for the sensitivity of the information or type of safeguard such as "Solicitor-client privilege", "Third Party Commercial Information", "Staff Relations", etc.;
- The suffix "A" after the word Protected for low-sensitive information;
- The suffix "B" after the word Protected for particularly sensitive information; and
- The suffix "C" after the word Protected for extremely sensitive information.

Confidential Records Marking

- Upper right corner of the face of the document; and
- Control copies in the same way as secret documents when warranted by a Threat and Risk Assessment (TRA).

Secret Records Marking

- Upper right corner of each page;
- Show the total number of pages on each page;
- Unique whole number to each copy; and
- Mark the copy number on each page and maintain a distribution list.

Top Secret Records Marking

- Upper right corner of each page and show the total number of pages on each page;
- Unique whole number to each copy;
- Mark the copy number on each page and maintain a distribution list; and
- Additional copies may be made only if an identifying number is assigned and a distribution list is maintained.

d. ***Marking Covering Letters and Other Transmittal Documents***
Covering letters and other transmittal documents should be marked:

- "Unclassified without attachment(s)" or
- "Unprotected without attachment(s).

e. ***Printed Forms and Questionnaires***
Printed forms and questionnaires that do not require protection until completed should have the security marking printed in accordance with the following examples:

- Protected A, B or C (as the case may be) (when completed); and
- Secret (when completed).

f. ***Drafts, Note Books and Appendices and Other Attachments***
These documents must each bear the relevant security marking until they are disposed of in the appropriate manner.

g. ***Microforms***
The containers for microfiche and microfilms must bear the appropriate security marking and the microfiches must be marked on the header line as well.

h. ***Electronic Information***
The container must be marked appropriately, and the classification or protection shall be clearly stated on each record.

i. ***Computer Printouts***

Computer printouts must show the appropriate security marking at the top of each page

j. ***Voice and Audiotape Recordings***
The container must be marked appropriately, and the classification or protection shall be clearly stated at the beginning and at the end of the recording.

k. ***Other physical medium***
Efforts must be made to meet the objective of the "eye-visibility" of the security marking for all other physical types of records, keeping in mind the practicability of such measure. When in doubt, managers and employees should contact the Security Services Directorate for advice.

Length of Time Information is Considered Sensitive

Sensitive information must be categorized only for the time it requires protection, after which it is to be declassified or downgraded". Declassifying information means removing the classification, whereas downgrading information means reducing the Protection level of a record or removing the protection entirely.

The moment for the declassification or downgrading is usually determined at the time of the creation of the record and it is set for a pre-determined date. Sometimes, circumstances will dictate the appropriate time for the declassification or downgrading. Examples of such circumstances include:

- Publication by the department of a press communiqué on the subject or issue or disclosure of the information by the Minister in the House of Commons;
- Before disclosing under ATIP. The declassification or downgrading may apply only to the part of the record that is to be disclosed to an applicant under the Act;
- Disclosure of personal information under the Privacy Act to the individual to whom the information relates. The disclosure of personal information about an individual to that individual does not affect the status of the information as protected because the department must still prevent other individuals from having access to the information; and
- Disclosure of commercial information of a third party to that same third party under the Access to Information Act. The disclosure of the commercial information in that context does not affect the status of the information as protected because the department must still prevent other individuals and legal entities from having access to it.

Declassifying or Downgrading of Information

The authority for the declassification or downgrading of information lies with the originator of the document. The term "originator" means:

- The individual who created the document;
- The individual who obtained the record or the information; or
- The unit where the individual who created the document or who obtained it worked at that time.

Where the originator is no longer available, the unit that has legal control over the document or that is currently responsible for the function of the originating unit will be responsible for its declassification or downgrading. If no one is responsible for the function, the local records office will then assume responsibility for the process.

Originators from other institutions must be consulted before information is declassified or downgraded. The consultation may be done verbally or in writing.

Indicating the Declassification or the Downgrading on the Record

Declassified and downgraded records must be marked as follows:

- "Declassified" or "Downgraded";
- The date of the declassification or downgrading;
- The identity of the manager or employee who declassified or downgraded the record.

The Need to Know Principle

Managers and employees are not entitled to access information merely because of their status, rank or office. They must request access only to the information for which they have an absolute need in order to perform their duties. The need to know is usually established by determining if the operational or administrative objective could be achieved without gaining access to the information. The key is to reach a balance between the administrative or operational requirements and the consequences that could flow from the manager or the employee gaining access to the information (i.e., embarrassment for the individual the information is about, relative loss of confidentiality for third party business information, etc.).

Access to Classified Information

Access to classified Information shall be limited to individuals who:

- Have a legitimate or legal right to know;

and who

- Have the proper security clearance.

The security clearance required for each level of classified information is as follows:

Confidential	Level 1 Security Clearance
Secret	Level 2 Security Clearance
Top Secret	Level 3 Security Clearance

Custodians of classified information are responsible for ensuring compliance with the above requirements before granting access to such information.

Access to Protected Information

Access to protected Information shall be limited to individuals who:

- Have a legitimate or legal right to know;

and who

- Have a reliability status. A reliability status is the minimum security level to work for Industry Canada.

Custodians of protected information are responsible for ensuring compliance with the above requirements before granting access to such information.

Transport and Transmittal of Sensitive Information

Please refer to the IC pamphlet entitled "Guide to the Transmission, Storage and Destruction of Protected and Classified Information".

A Guide to the Transmission, Storage and Destruction of Protected and Classified Information

http://icintra.ic.gc.ca/security-securite/

(Français au verso)

Security Services Directorate

Rev. 01/04

Canada

PROTECTED A

Unauthorized release could cause injury to an individual, organization or government.

- Loss of Privacy
- Embarrassment

EXAMPLES:

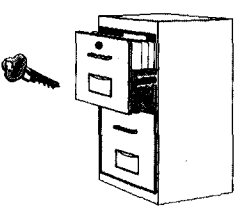
- Unsolicited Proposals
- Date of Birth
- Home addresses and telephone numbers
- Salaries

Mark Document/Data: PROTECTED A

Storage:
– Container with keyed lock in an operations zone
– Locked office

Electronic Storage:
– Hard drive with password
– Network drive (for authorized users only)
– Portable media in a container with keyed lock

Transmittal:
– Unmarked single envelope
– Internal and 1st class mail



Electronic Transmission:
– Internal network and mail
– Regular fax

Destruction:
– Hand shred and recycle

Electronic Destruction:
– Delete and empty recycle bin

Security Screening:
– Reliability status

**Portable media including hard disks may require physical destruction (contact IT Security)*

PROTECTED B

Unauthorized release could cause serious injury to an individual, organization or government.

- Prejudicial treatment
- Loss of reputation or competitive edge

EXAMPLES:

- Competitive position of a third party
- Criminal information on an individual
- Performance evaluations
- Financial, religious or political beliefs
- Information received "in confidence" from other government organizations

Mark Document/Data: PROTECTED B

Storage:
– Approved security container with approved combination lock in an operations zone

Electronic Storage:
– Portable media in an approved security container
– Encrypted

Transmittal:
– Mark inner envelope "Protected B"
- "to be opened by addressee only"
– Unmarked outer envelope
– Internal and 1st class mail

Electronic Transmission:
– PKI encryption
– Secure fax (connected to a STU III Telephone)

Destruction:
– Approved machine shredder and recycle

Electronic Destruction:
– *Delete securely with an approved disk sanitization utility (contact IT Security)

Security Screening:
– Reliability status

PROTECTED C

Unauthorized release could cause extremely serious injury to an individual, organization or government.

- Significant financial loss
- Loss of life

EXAMPLES:

- Information that could cause the bankruptcy of an individual or company
- Testimony against another individual

Mark Document/Data: PROTECTED C

Storage:
– Approved security container with approved combination lock in an operations zone

Electronic Storage:
– Portable media in an approved security container

Transmittal:
– Mark inner envelope "Protected C" - "to be opened by addressee only", enclose "Transmittal Note and Receipt" form
– Unmarked outer envelope
– Internal and 1st class mail

Electronic Transmission:
– Secure fax (connected to a STU III Telephone)

Destruction:
– Approved machine shredder and recycle

Electronic Destruction:
– *Delete securely with an approved disk sanitization utility (contact IT Security)

Security Screening:
– Reliability status

CONFIDENTIAL

Unauthorized release could cause injury to the national interest.

Mark Document/Data: CONFIDENTIAL

Storage:
– Approved security container with approved combination lock in an operations zone

Electronic Storage:
– Portable media in an approved security container

Transmittal:
– Unmarked single envelope
– Internal and 1st class mail

Electronic Transmission:
– Secure fax (connected to a STU III Telephone)

Destruction:
– Approved machine shredder and recycle

Electronic Destruction:
–*Delete securely with an approved disk sanitization utility (contact IT Security)

Security Clearance:
– Confidential

SECRET

Unauthorized release could cause serious injury to the national interest.

Mark Document/Data: SECRET

Storage:
– Approved security container with approved combination lock in an operations zone

Electronic Storage:
– Portable media in an approved security container

Transmittal:
– Mark inner envelope "Secret" - "to be opened by addressee only"
– Unmarked outer envelope
– Internal mail
– Within Canada, deliver by hand or courier service (proof of mailing)
– Outside Canada delivery by Diplomatic Security Mail Service

Electronic Transmission:
– Secure fax (connected to a STU III Telephone)

Destruction:
– Approved machine shredder and recycle

Electronic Destruction:
–*Delete securely with an approved disk sanitization utility (contact IT Security)

Security Clearance: Secret

TOP SECRET

Unauthorized release could cause extremely serious injury to the national interest.

Mark Document/Data: TOP SECRET

Storage:
– Approved dial safe in a security zone

Electronic Storage:
– Portable media in a dial safe in a security zone

Transmittal:
– Mark inner envelope "Top Secret" - "to be opened by addressee only" with "Transmittal note and Receipt" form, tape sealed
– Unmarked outer envelope
– Deliver by hand (receipt signature) **only**
– Outside Canada delivery by Diplomatic Security Mail Service

Electronic Transmission:
– Secure fax (connected to a STU III Telephone)

Destruction:
– Approved machine shredder and recycle

Electronic Destruction:
– Contact IT Security for directives

Security Clearance: Top Secret

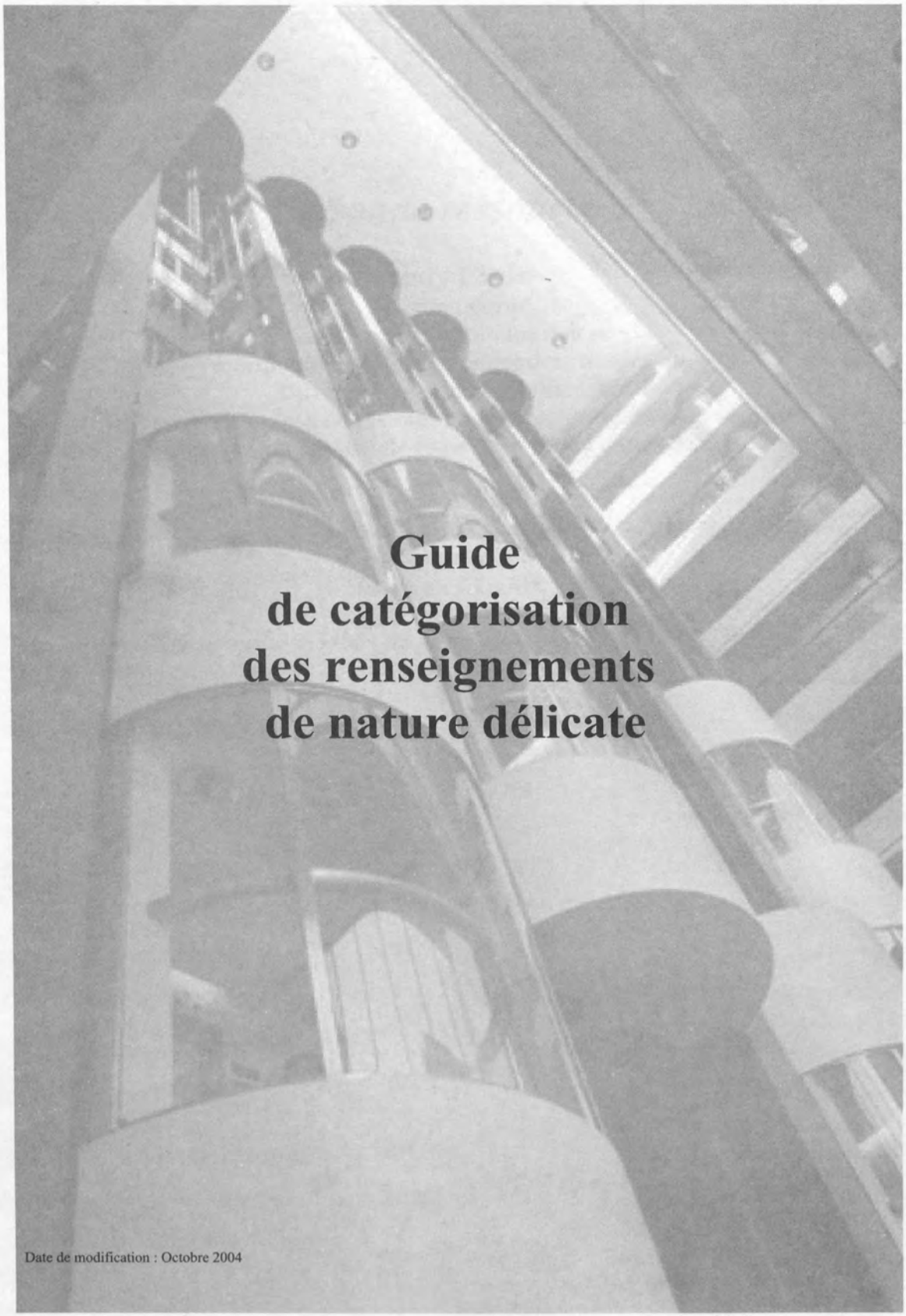
CLASSIFIED INFORMATION

Includes documents such as those concerned with:

- Federal-provincial relations
- International affairs
- Defence or the economic interests of Canada
- Cabinet Papers
- Advice and recommendations connected with the above information
- Information involving security and intelligence or security assessment

Industrie Canada Industry Canada

Canada



Guide de catégorisation des renseignements de nature délicate

Date de modification : Octobre 2004

Personne ressource :

Sandy Little
Gestionnaire
Formation et sensibilisation et
coordination régionales en matière de sécurité
Direction des services de sécurité
Direction générale des systèmes financiers, installations et sécurité
Secteur de la Fonction de contrôleur et de l'administration

Édifice C.D. Howe
Pièce 327A - Tour est
235, rue Queen
Ottawa - K1A 0H5

Téléphone : (613) 954-4358 ❖Télécopieur : (613)941-2380

Courriel : little.sandy@ic.gc.ca

TABLE DES MATIÈRES

Pages

Processus de catégorisation des renseignements de nature délicate

La catégorisation des renseignements de nature délicate identifie le niveau de sensibilité des renseignements ministériels. L'initiateur du document doit déterminer le niveau de sensibilité. Il existe deux types de niveaux de sensibilité : renseignement protégé et renseignement classifié.

Différence entre la « *classification* » et la « *protection* » des *renseignements*

La « ***classification*** » des renseignements est le processus qui consiste à déterminer que la nature délicate des renseignements est telle que leur divulgation, leur modification ou leur destruction non autorisée nuirait à la sécurité nationale ou à l'intérêt national. Par « sécurité nationale » et « intérêt national », nous entendons la stabilité politique, sociale ou économique à laquelle pourrait nuire la divulgation, la modification ou la destruction non autorisée des renseignements. L'indication sur les dossiers classifiés de la mention « Confidentiel », « Secret » ou « Très secret » facilite leur identification et fait en sorte qu'ils soient traités de la manière qui convient à leur niveau de nature délicate. Voici des exemples de renseignements classifiés :

- documents confidentiels du Cabinet (documents confidentiels du Conseil privé de la Reine pour le Cabinet), y compris les présentations au Conseil du Trésor;
- renseignements relatifs aux opérations de renseignements militaires et anti-terroristes;
- renseignements stratégiques intéressant les négociations commerciales internationales et d'autres manifestations et activités internationales pouvant toucher aux intérêts du Canada ou de ses alliés;
- renseignements pouvant compromettre l'intégrité des institutions démocratiques du Canada;
- renseignements pouvant nuire à la capacité du gouvernement du Canada à gérer l'économie nationale (décisions macroéconomiques); et
- renseignements visés par le secret professionnel des avocats touchant la sécurité nationale ou l'intérêt national.

En raison de la nature de ses activités, seule une petite partie des renseignements d'Industrie Canada est classifiée.

La « ***protection*** » des renseignements est le processus qui consiste à déterminer que des renseignements qui ne touchent pas la sécurité nationale ou l'intérêt national sont néanmoins de nature délicate et méritent d'être protégés. Les dossiers qui renferment des renseignements protégés doivent porter la mention « Protégé A », « Protégé B » ou « Protégé C », selon leur niveau de nature délicate. Bien que les renseignements appartenant à certaines des catégories suivantes soient parfois qualifiés de « classifiés » en raison de circonstances exceptionnelles, ils sont généralement considérés comme « protégés » :

- secrets commerciaux et renseignements commerciaux, financiers, techniques et scientifiques de tiers;

- renseignements personnels qui permettent d'identifier la personne visée, y compris l'adresse et le numéro de téléphone à domicile, des identificateurs personnels comme le numéro d'assurance sociale, des documents d'évaluation du rendement, des renseignements médicaux et des casiers judiciaires;
- renseignements obtenus à titre confidentiel d'administrations provinciales et municipales;
- documents et dossiers d'enquête de la police;
- renseignements relatifs à la négociation de subventions et d'une aide technique destinées aux entreprises;
- plans de gestion du personnel;
- comptes rendus de consultations et de délibérations auxquelles participent des agents et des employés du Ministère ou des membres du personnel du Ministre;
- plans de communications sur les activités du Ministère; et
- renseignements visés par le secret professionnel des avocats qui ne touchent pas la sécurité nationale ou l'intérêt national.

Procédures spéciales de traitement des documents du Cabinet

Le gouvernement du Canada administre par la voie d'un Cabinet. Ainsi, la responsabilité ne repose pas sur un seul ministre mais sur l'ensemble des ministres qui font partie du Cabinet. Les ministres du Cabinet ont une responsabilité collective envers toutes les mesures prises par le Cabinet et doivent appuyer toutes les décisions de ce dernier, qu'ils soient directement concernés ou non et qu'ils aient été d'accord ou non à l'origine. Cependant, pour être en mesure de prendre une décision définitive, tous les ministres doivent pouvoir s'exprimer librement au cours des discussions menant aux décisions du Cabinet. Si ces délibérations étaient publiques, la responsabilité collective des ministres en serait diminuée. Cette règle protège donc le principe de la responsabilité collective des ministres, car elle permet à ces derniers d'appuyer les décisions du gouvernement quelles que soient leurs opinions personnelles. Elle permet aussi aux ministres de participer à des débats francs qui sont essentiels au fonctionnement efficace de ce genre de régime.

Pour préserver la confidentialité essentielle au fonctionnement efficace du Cabinet, le législateur a prévu au paragraphe 69 (1) de la *Loi sur l'accès à l'information* et au paragraphe 70 (1) de la *Loi sur la protection des renseignements personnels* que les documents confidentiels du Conseil privé de la Reine pour le Canada étaient soustraits au champ d'application de ces lois. Cela signifie qu'il n'est pas nécessaire de communiquer des documents du Cabinet en réponse à une demande d'accès présentée en vertu de la *Loi sur l'accès à l'information* ou la *Loi sur la protection des renseignements personnels.* Le Bureau du Conseil privé (BCP) est définitivement habilité à déterminer si un document constitue un document du Cabinet au sens de ces lois; une

procédure de consultation a été établie pour permettre aux responsables de l'application de ces lois dans les ministères fédéraux de confirmer auprès du BCP que des documents constituent des documents du Cabinet et d'entreprendre un processus de consultation avec le BCP. Il est important de signaler qu'à Industrie Canada, l'unité de l'accès à l'information est responsable de déterminer si un document constitue un document du Cabinet et d'initier le processus de consultation avec le BCP. **Par conséquent, tous les documents du Cabinet dont on demande la communication aux termes de la *Loi sur l'accès à l'information* ou la *Loi sur la protection des renseignements personnels* doivent être envoyés à l'unité responsable de leur application.**

Selon la Politique du gouvernement sur la sécurité (PGS), les documents renfermant des renseignements visés par le paragraphe 69 (1) de la *Loi sur l'accès à l'information* et le paragraphe 70 (1) de la *Loi sur la protection des renseignements personnels* doivent être classifiés, dans l'intérêt national, et doivent à tout le moins porter la cote « Secret ».

Types de renseignements qui ne sont ni classifiés ni protégés

Les renseignements appartenant aux catégories suivantes ne sont généralement ni classifiés ni protégés :

- renseignements publiés ou offerts en vente au public;
- renseignements affichés sur le site Internet du Ministère;
- renseignements conservés dans les registres publics du Ministère;
- renseignements divulgués en application de la *Loi sur l'accès à l'information* par l'autorité compétente du Ministère;
- politiques et procédures ministérielles employées par les employés dans l'exercice de leurs fonctions;
- renseignements budgétaires du Ministère; et
- renseignements sur les subventions et les contrats, à l'exception des renseignements exclusifs que renferme le dossier d'un contrat.

En outre, toujours d'après la PGS, la classification et la protection des renseignements ne doivent pas servir illégalement à protéger des renseignements sur des actes frauduleux ou malveillants.

Divulgation des renseignements classifiés ou protégés en vertu de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*

En conformité avec le principe selon lequel les lois ont préséance sur les politiques et les procédures, la décision de refuser l'accès à des renseignements demandés en vertu de la LAI ou de la LPRP est assujettie uniquement aux dispositions d'exemption et d'exclusion de ces deux lois. La cote de sécurité d'un document n'entre donc pas en ligne de compte. Cependant, les renseignements à divulguer en vertu de ces lois doivent tout d'abord être déclassés ou

déclassifiésavant de pouvoir être divulgués, de façon à être soustraits à l'application des mesures de sécurité prévues par la PGS; et l'initiateur du document doit participer à ce processus. Nous reviendrons d'ici la fin de cette partie sur le processus de déclassement ou de déclassification.

Étapes de catégorisation des documents et d'une cote de sécurité

Le processus de catégorisation et d'inscription de la cote comporte les étapes suivantes :

Première étape :

Les renseignements ont-ils trait à l'intérêt national ou à la sécurité nationale?

Deuxième étape :

Dans l'affirmative, la perte temporaire ou permanente de confidentialité, d'intégrité ou de disponibilité des renseignements serait-elle préjudiciable, au sens des dispositions sur l'exemption ou l'exclusion de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels*?

Troisième étape :

Détermination de la gravité du préjudice causé à l'intérêt national ou à la sécurité nationale :

- pour tout autre préjudice, il faut inscrire sur le document la cote « **Confidentiel** ».
- s'il s'agit d'un préjudice grave, il faut inscrire sur le document la cote « **Secret** »;
- s'il s'agit d'un préjudice exceptionnellement grave, il faut inscrire sur le document la cote « **Très secret** ».

Quatrième étape :

Si les renseignements ne concernent par l'intérêt national ou la sécurité nationale, est-ce que la perte permanente ou temporaire de leur confidentialité, intégrité ou disponibilité entraînerait un autre type de préjudice, au sens des dispositions sur l'exclusion ou l'exemption de la *Loi sur l'accès à l'information* ou la *Loi sur la protection des renseignements personnels*?

Cinquième étape :

Dans l'affirmative, il faut déterminer si cette compromission causerait :

- un préjudice, et inscrire alors sur le document la cote « **Protégé A** ».
- un préjudice grave, et inscrire alors sur le document la cote « **Protégé B** »;
- un préjudice extrêmement grave, et inscrire alors sur le document la cote « **Protégé C** »;

Inscription de la cote de sécurité

Les exigences suivantes s'appliquent à l'inscription de la cote de sécurité sur les documents :

a. **La cote doit correspondre au niveau des renseignements les plus délicats que renferme le document.**
Autrement dit, la cote de sécurité doit correspondre au niveau des renseignements les plus délicats que le document renferme de façon à protéger les renseignements les plus délicats. Ainsi, un document qui renferme des renseignements justifiant la cote « Secret » et des renseignements justifiant la cote « Protégé B » doit porter la cote « Secret » comme s'il ne renfermait que ce genre de renseignements de façon que ceux-ci soient convenablement protégés.

b. **La cote doit être bien visible**
La cote doit être bien visible de façon que les gestionnaires et les employés puissent reconnaître un document de nature délicate simplement en y jetant un coup d'oeil. Bien que la visibilité de la cote puisse accroître la vulnérabilité d'un document si celui-ci est laissé sans surveillance dans un endroit public, elle vise à inciter les gestionnaires et employés à être plus vigilants dans le traitement de ces documents.

c. **La cote doit être inscrite à un endroit précis du document, et la circulation de celui-ci est assujettie à certaines règles.**

Inscription d'une cote sur les documents protégés.

- « Protégé » dans le coin supérieur droit de la première page du document;
- indication de la raison de la nature délicate des renseignements ou du type de précaution, p. ex. « secret professionnel des avocats », « renseignements commerciaux de tiers », « relations du personnel », etc.;
- le suffixe « A » après le mot « Protégé » pour les renseignements délicats.
- le suffixe « B » après le mot « Protégé » pour les renseignements particulièrement délicats;
- le suffixe « C » après le mot « Protégé » pour les renseignements extrêmement délicats;

Inscription d'une cote « Confidentiel »

- dans le coin supérieur droit de la première page du document; et
- suivi des copies de la même manière que pour les documents portant la cote « Secret » lorsque l'Évaluation de la menace et des risques (ÉMR) le justifie.

Inscription d'une cote « Secret »

- dans le coin supérieur droit de chaque page;
- indication du nombre total de pages sur chaque page;
- indication d'un nombre entier sur chaque copie; et
- indication du nombre de copies sur chaque page et tenue d'une liste de destinataires.

Inscription d'une cote « Très secret » :

- dans le coin supérieur droit de chaque page, avec indication du nombre total de pages sur chaque page;
- indication d'un nombre entier sur chaque copie;
- indication du nombre de copies sur chaque page et tenue d'une liste de destinataires; et
- production de copies additionnelles uniquement si un nombre d'identification est attribué et qu'une liste de distribution est tenue.

d. **Inscription d'une cote sur les lettres d'accompagnement et autres documents de transmission**

Les lettres d'accompagnement et les autres documents de transmission doivent porter les mentions suivantes :

- « non classifié sans les pièces jointes »; ou
- « non protégé sans les pièces jointes ».

e. **Formulaires ou questionnaires imprimés**

Les formulaires et questionnaires qui n'ont besoin d'être protégés qu'après avoir été remplis doivent porter une cote de sécurité comme les suivantes :

- Protégé A, B ou C (selon le cas) (une fois rempli); et
- Secret (une fois rempli).

f. **Ébauches, carnets de notes, annexes et autres pièces jointes**

Ces documents doivent tous porter la cote de sécurité applicable tant qu'ils n'ont pas été aliénés de la manière prévue.

g. **Microformes**

Les contenants de microfiches et de microfilms doivent porter la cote de sécurité applicable; la cote doit aussi être inscrite sur la ligne d'en-tête des microfiches.

h. **Renseignements sous forme électronique**

Le contenant doit porter la cote voulue, et la protection ou classification doit figurer clairement sur chaque document.

i. **Imprimés d'ordinateur**

La cote de sécurité voulue doit figurer dans la partie supérieure de chaque page des imprimés d'ordinateur.

j. **Enregistrements audiovisuels et sur bandes magnétiques**

La cote doit être inscrite sur le contenant, et la classification ou protection doit être bien indiquée au début et à la fin de l'enregistrement.

k. **Autres supports matériels**

Dans la mesure du possible, il faut s'assurer que la cote de sécurité est bien visible sur les autres supports matériels tout en gardant le côté pratique de cette mesure en tête. En cas de doute, les gestionnaires et employés sont invités à demander des conseils à la Division des Services de sécurité.

Durée de validité de la classification des renseignements de nature délicate

Les renseignements de nature délicate doivent être catégorisés uniquement pendant qu'ils doivent être protégés; ils doivent ensuite être déclassifiés ou déclassés. Par déclassification, on entend l'élimination de la classification, tandis que dans le cas des déclassements, cela signifie de réduire ou d'éliminer complètement la protection.

La date de déclassification ou de déclassement est généralement déterminée au moment de la création du document et elle est prévue pour une date prédéterminée. Les circonstances déterminent parfois le moment auquel il convient de déclassifier des renseignements ou de les déclasser. Voici des exemples de ces circonstances :

- publication par le Ministère d'un communiqué sur le sujet ou divulgation des renseignements par le Ministre à la Chambre des communes;
- divulgation des renseignements aux termes de la LAI. La déclassification ou le déclassement peut s'appliquer uniquement à la partie du document qui sera communiquée au demandeur des renseignements;
- divulgation, en vertu de la *Loi sur la protection des renseignements personnels,* de renseignements personnels à la personne visée. La divulgation de renseignements personnels à la personne visée ne change pas le statut de renseignements protégés de ceux-ci étant donné que le Ministère doit empêcher d'autres personnes d'avoir accès à ces renseignements;
- divulgation de renseignements commerciaux d'un tiers à ce dernier en vertu de la *Loi sur l'accès à l'information.* La divulgation de renseignements commerciaux dans ce contexte ne change pas le statut de renseignements protégés de ceux-ci étant donné que le Ministère doit empêcher d'autres personnes et entités juridiques d'avoir accès à ces renseignements.

Déclassification ou déclassement des renseignements

Le pouvoir de déclassification ou de déclassement des renseignements appartient à l'initiateur du document. Le mot « initiateur » signifie :

- la personne qui a créé le document;
- la personne qui a obtenu le document ou les renseignements; ou

  l'unité où travaillait la personne qui a créé ou obtenu le document.

Si l'initiateur n'est plus disponible, l'unité qui exerce le contrôle juridique sur le document ou la fonction de l'unité initiale est chargée de la déclassification ou du déclassement. Si personne n'est chargé de cette fonction, le bureau local des documents assumera la responsabilité du processus.

Il faut consulter de vive voix ou par écrit les initiateurs d'autres institutions avant de déclassifier ou de déclasser des renseignements.

Indication de la déclassification ou du déclassement sur le document

Les documents déclassifiés ou déclassés doivent porter les indications suivantes :

« déclassifié » ou « déclassé »;

- la date de la déclasssification ou du déclassement;
- l'identité du gestionnaire ou de l'employé qui a déclassifié ou déclassé le document.

Le principe du besoin de savoir

Les gestionnaires et les employés ne jouissent pas du droit d'accès aux renseignements simplement en raison de leurs statut, rang ou fonctions. Ils doivent demander l'accès uniquement aux renseignements dont ils ont absolument besoin pour exercer leurs fonctions. On détermine ordinairement le besoin de savoir en voyant s'il est possible d'atteindre l'objectif opérationnel ou administratif sans avoir accès aux renseignements. Il s'agit de trouver un juste milieu entre les exigences administratives ou opérationnelles et les conséquences pouvant découler de l'accès par le gestionnaire ou l'employé aux renseignements (p. ex. situation gênante pour la personne visée par les renseignements, perte de confidentialité des renseignements commerciaux de tiers).

Accès aux renseignements classifiés

Peuvent avoir accès aux renseignements classifiés, uniquement les personnes qui :

- ont légitimement ou légalement le droit de les connaître,

et qui

- possèdent une attestation de sécurité voulue.

L'attestation de sécurité exigée pour chaque niveau de renseignements classifiés est la suivante :

Confidentiel	Attestation de sécurité niveau 1
Secret	Attestation de sécurité niveau 2
Très secret	Attestation de sécurité niveau 3

Les gardiens des renseignements classifiés doivent assurer la conformité avec ces exigences avant d'accorder l'accès à ceux-ci.

Accès aux renseignements protégés

Ont accès aux renseignements Protégés, les personnes qui :

- ont légitimement ou légalement le droit de les connaître,

et qui

- ont la cote de fiabilité. Cette cote correspond au niveau de sécurité minimal requis pour travailler à Industrie Canada.

Les gardiens des renseignements protégés doivent assurer la conformité avec ces exigences avant d'accorder l'accès à ceux-ci.

Transport et transmission des renseignements de nature délicate

Veuillez consulter la brochure d'IC intitulé « Guide pour la transmission, l'entreposage et la destruction de renseignements protégés et classifiés. »

Un guide pour la transmission, l'entreposage et la destruction de renseignements protégés et classifiés

http://icintra.ic.gc.ca/security-securite/

(English on reverse)

Direction des services de sécurité

Rev. 01/04

Canada

PROTÉGÉ A

Une divulgation non autorisée pourrait causer un préjudice à un particulier, à un organisme ou au gouvernement.

- Atteinte à la vie privée
- Embarras

EXEMPLES :

- Propostions spontanées
- Date de naissance
- Adresses et numéros de téléphone résidentiels
- Les salaires

Marquer document/données : PROTÉGÉ A

Entreposage :
– Classeur verrouillé à clé dans une zone d'opérations
– Bureau verrouillé

Archivage électronique :
– Disque dur avec mot de passe
– Lecteur réseau « pour utilisateurs autorisés seulement »
– Support portatif dans un classeur verrouillé à clé

Transmission :
– Enveloppe simple non marquée
– Courrier interne et de 1re classe

Transmission électronique :
– Réseau interne et courrier
– Télécopieur ordinaire

Destruction :
– Déchiquetage manuel et recyclage

Destruction électronique :
– Supprimer et vider la corbeille

Autorisation de sécurité :
– Cote de fiabilité

PROTÉGÉ B

Une divulgation non autorisée pourrait causer un grave préjudice à un particulier, à un organisme ou au gouvernement.

- Traitement préjudiciable
- Atteinte à la réputation ou perte d'un avantage concurrentiel

EXEMPLES :

- Position concurrentielle d'un tiers
- Information criminelle sure une personne
- Financier, croyances religieuses ou politiques d'une personne
- Évaluations de rendement
- Information reçue à titre confidentiel d'autres organisations gouvernementales

Marquer document/données : PROTÉGÉ B

Entreposage :
– Classeur de sécurité approuvé, doté d'un cadenas à combinaison approuvé, dans une zone d'opérations

Archivage électronique :
– Support portatif placé dans un classeur de sécurité approuvé
– Chiffré

Transmission :
– Enveloppe intérieure marquée « Protégé B » - « À être ouverte par le destinataire uniquement »
– Enveloppe éxterieure non marquée
– Courrier interne et de 1re classe

Transmission électronique :
– Chiffrement ICP
– Télécopieur sécuritaire « par l'entremise d'un téléphone STU-III »

Destruction :
– Déchiqueteuse approuvée et recyclage

Destruction électronique :
– *Supprimer de façon sûre avec une disquette approuvée d'un programme utilitaire d'expurgation « communiquer avec la Sécurité en TI »

Autorisation de sécurité : Cote de fiabilité

PROTÉGÉ C

Une divulgation non autorisée pourrait causer un préjudice extrêmement grave à un particulier, à un organisme ou au gouvernement.

- Perte d'argent considérables
- Perte de vie

EXEMPLES :

- De l'information qui pourrait causer la faillite d'une personne ou d'une organisation
- Témoignage contre une autre personne

Marquer document/données : PROTÉGÉ C

Entreposage :
– Classeur de sécurité, doté d'un cadenas à combinaison approuvé, dans une zone d'opérations

Archivage électronique :
– Support portatif dans un classeur de sécurité approuvé

Transmission :
– Enveloppe intérieure marquée « Protégé C » et « À être ouverte par le destinataire uniquement », accompagnée du formulaire Note d'envoi et reçu
– Enveloppe éxterieure non marquée
– Courrier interne et de 1re classe

Transmission électronique :
– Télécopieur sécuritaire (par l'entremise d'un téléphone « STU III »

Destruction :
– Déchiqueteuse approuvée et recyclage

Destruction électronique :
– *Supprimer de façon sûre avec une disquette approuvée d'un programme utilitaire d'expurgation « communiquer avec la Sécurité en TI »

Autorisation de sécurité : Cote de fiabilité

**Supports portables, incluant les lecteurs de disques dur, peuvent exiger la destruction physique « communiquer avec la Sécurité en TI »*

CONFIDENTIEL

Une divulgation non autorisée pourrait causer un préjudice à l'intérêt national.

Marquer document/données : CONFIDENTIEL

Entreposage :
– Classeur de sécurité approuvé, doté d'un cadenas à combinaison approuvé, dans une zone d'opérations

Archivage électronique :
– Support portatif placé dans un classeur de sécurité approuvé

Transmission :
– Enveloppe simple non marquée
– Courrier interne et de 1re classe

Transmission électronique :
– Télécopieur sécuritaire « par l'entremise d'un téléphone STU-III »

Destruction :
– Déchiqueteuse approuvée et recyclage

Destruction électronique :
– Communiquer avec la Sécurité en TI

Autorisation de sécurité :
– Confidentiel

SECRET

Une divulgation non autorisée pourrait causer un grave préjudice à l'intérêt national.

Marquer document/données : SECRET

Entreposage :
– Classeur de sécurité approuvé, doté d'un cadenas à combinaison approuvé, dans une zone d'opérations

Archivage électronique :
– Support portatif placé dans un classeur de sécurité approuvé

Transmission :
– Enveloppe intérieure marquée « Secret » et « À être ouverte par le destinataire uniquement »
– Enveloppe éxterieur non marquée
– Courrier interne
– Au Canada : par porteur ou service de messagerie « preuve d'expédition »
– À l'extérieur du Canada : par service de courrier diplomatique de sécurité

Transmission électronique :
– Télécopieur sécuritaire « par l'entremise d'un téléphone STU-III »

Destruction :
– *Supprimer de façon sûre avec une disquette approuvée d'un programme utilitaire d'expurgation « communiquer avec la Sécurité en TI »

Destruction électronique :
– Transmission du support, par porteur, à Sécurité de la TI

Autorisation de sécurité : Secret

TRÈS SECRET

Une divulgation non autorisée pourrait causer un préjudice extrêmement grave à l'intérêt national.

Marquer document/données : TRÈS SECRET

Entreposage :
– Coffre-fort à combinaison approuvé dans une zone de sécurité

Archivage électronique :
– Support portatif placé dans un coffre-fort à combinaison dans une zone de sécurité

Transmission :
– Enveloppe intérieure marquée « Très secret » et « À être ouverte par le destinataire uniquement », accompagnée du formulaire Note d'envoi et reçu, et sceller avec du ruban
– Enveloppe éxterieur non marquée
– Par porteur **seulement** « reçu signé »
– À l'extérieur du Canada : par service de courrier diplomatique de sécurité

Transmission électronique :
– Télécopieur sécuritaire « par l'entremise d'un téléphone STU-III »

Destruction :
– Déchiqueteuse approuvée et recyclage

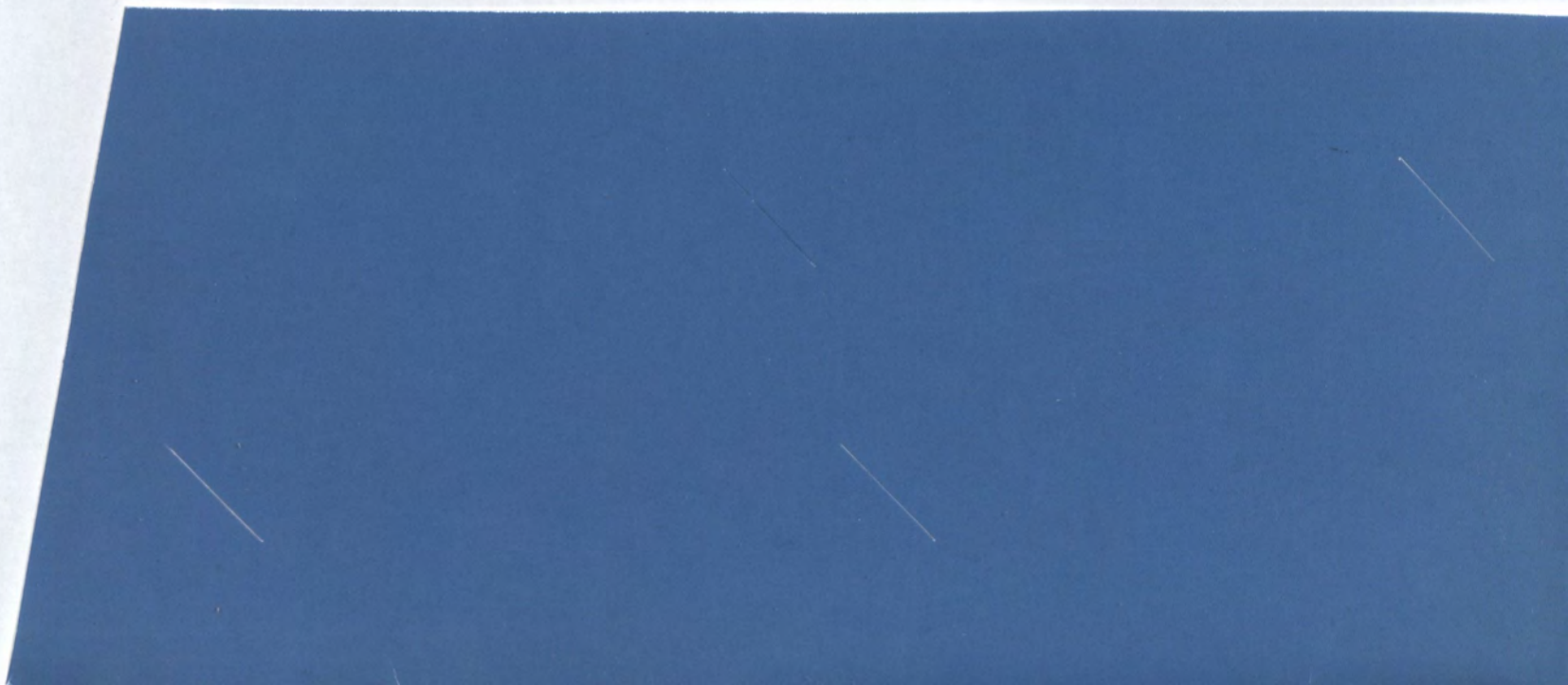
Destruction électronique :
– Transmission du support, par porteur, à Sécurité de la TI

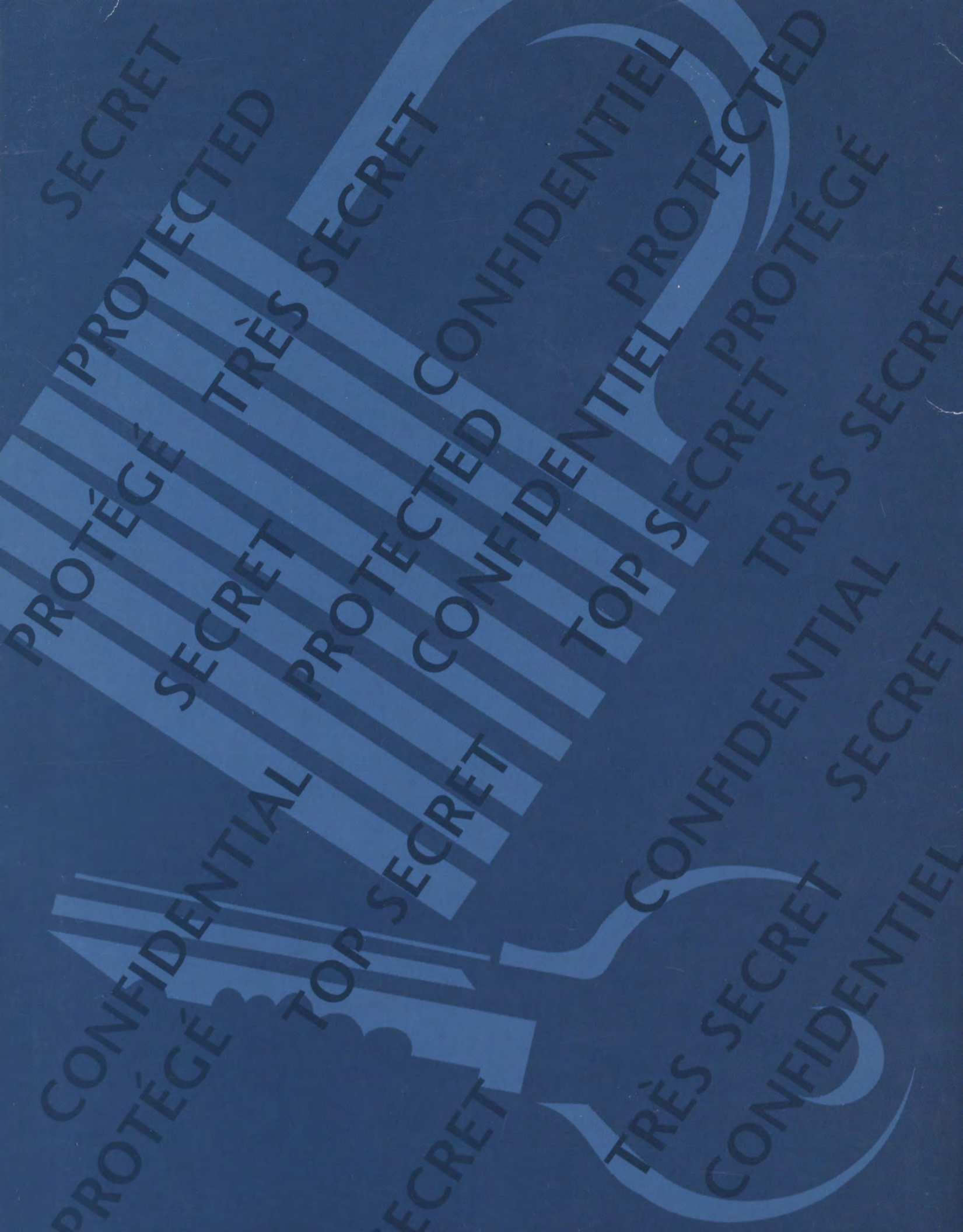
Autorisation de sécurité : Très secret

RENSEIGNEMENTS CLASSIFIÉS

Ceci comprend les documents qui traitent, entre autres, des sujets suivants :

- Relations fédérales-provinciales
- Affaires internationales
- Défense ou intérêts économiques du Canada
- Dossiers du Cabinet
- Conseils et recommandations liés aux renseignements ci-dessus
- Renseignements concernant la sécurité, les services de renseignements ou les enquêtes de sécurité




SECRET
PROTECTED
PROTÉGÉ
TRÈS SECRET
SECRET
CONFIDENTIAL
PROTECTED
CONFIDENTIEL
TOP SECRET
SECRET
CONFIDENTIAL
PROTÉGÉ
TOP SECRET
TRÈS SECRET
CONFIDENTIAL
SECRET
TRÈS SECRET
CONFIDENTIEL